

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MARC OPPERMAN, et al.,

Plaintiffs,

v.

PATH, INC., et al.,

Defendants.

Case No. 13-cv-00453-JST

**ORDER GRANTING IN PART AND DENYING IN PART
DEFENDANTS' MOTIONS TO DISMISS**

Re: ECF Nos. 393, 394, 395, 396

THIS DOCUMENT RELATES TO ALL CASES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

United States District Court
Northern District of California

I.	Background	1
A.	The App Store	3
B.	The Subject Apps	5
C.	Apple's Representations.....	7
II.	Legal Standards	8
III.	Apple's Motion to Dismiss	10
A.	Article III Standing.....	10
B.	Communications Decency Act.....	18
C.	Misrepresentation Claims.....	23
D.	California Comprehensive Computer Data Access and Fraud Act	34
E.	Strict Products Liability: Design Defect and Failure to Warn	36
F.	Negligence.....	37
G.	RICO	37
H.	Aiding and Abetting	37
IV.	App Defendants' Motions to Dismiss	38
A.	Article III Standing.....	38
B.	Plaintiffs' UCL Claims	41
C.	Invasion of Privacy: Intrusion Upon Seclusion.....	41
D.	Invasion of Privacy: Public Disclosure of Private Facts	47
E.	CDAFA and Computer Fraud and Abuse Act	48
F.	Electronic Communications Privacy Act	48
G.	Texas and California Wiretap Statutes.....	49
H.	Texas Theft Liability Act	50
I.	RICO and Vicarious Liability	50
V.	Facebook and Gowalla's Motion to Dismiss	50
A.	Uniform Fraudulent Transfer Act.....	51
B.	Successor Liability	53
C.	Aiding and Abetting	54
VI.	Conclusion.....	55

Before the Court are four motions to dismiss filed by Defendants in this action. The operative Consolidated Amended Class Action Complaint (“CAC”), ECF No. 362, collects the claims of fifteen plaintiffs¹ in four related actions against a total of fifteen Defendants. Defendant Apple Inc. designs and manufactures the iPhone, the iPod touch, and the iPad, (“iDevices”), each of which is a mobile device that can wirelessly access the Internet. Since 2008, those devices have included an App Store, which enables users to download software, or apps, to their devices created by third parties. Each Defendant except for Apple is an app developer² (collectively, “App Defendants”). Plaintiffs allege that the App Defendants’ apps have been surreptitiously stealing and disseminating the contact information stored by customers on Apple devices. CAC ¶ 7.

I. BACKGROUND

Plaintiffs bring this action on their own behalf, on behalf of an “iDevice Class,” composed of all purchasers of Apple’s iDevices between July 10, 2008 and the present who downloaded the App Defendants’ apps, and on behalf of three subclasses: the “Malware Subclass,” the “Address Book Subclass,” and the “Texas Subclass.” CAC ¶ 48. The Malware Subclass comprises those who downloaded the subject apps. The Address Book Subclass comprises those in the Malware Subclass whose iDevice, without requesting prior approval, “transmitted, disclosed, and/or disseminated the iDevice’s mobile address book (or substantial portions thereof) over the Internet and/or to third-parties” due to the subject apps.

The CAC asserts several overlapping claims against different Defendants on behalf of different Plaintiffs. In total, the CAC asserts the following statutory claims: violation of California’s Unfair Competition Law (“UCL”), Cal. Bus. & Prof.s Code § 17200, *et seq.*; violation

¹ The sixteenth Plaintiff, Haig Arabian, has voluntarily dismissed his claims. ECF No. 426. The remaining Plaintiffs are Alan Beuershasen, Giuli Biondi, Lauren Carter, Steve Dean, Stephanie Dennis-Cooley, Jason Green, Claire Hodgins, Gentry Hoffman, Rachelle King, Nirali Mandaywala, Claire Moses, Judy Paul, Maria Pirozzi, Theda Sandiford and Greg Varner.

² The App Defendants are: Chillingo Ltd. (*Angry Birds* and *Cut the Rope*), Electronic Arts, Inc., Facebook, Inc., Foodspotting, Inc., Foursquare Labs, Inc., Gowalla, Inc., Hipster, Inc., Instagram, Inc., Kik Interactive, Inc., Path, Inc., Rovio Entertainment, Ltd. (*Angry Birds Classic*), Twitter, Inc., Yelp!, Inc., and ZeptoLab UK Ltd. (*Cut the Rope*).

of California’s False and Misleading Advertising Law (“FAL”), Cal. Bus. & Prof.s Code § 17500, *et seq.*; violation of California’s Consumer Legal Remedies Act (“CLRA”), Cal. Civ. Code § 1750, *et seq.*; violation of the California Comprehensive Computer Data Access and Fraud Act (“CDAFA”), Cal. Pen. Code § 502; violation of California’s Wiretap / Invasion of Privacy Act, Cal. Pen. Code § 630, *et seq.*; violation of the Uniform Fraudulent Transfer Act, Cal. Civ. Code § 3439; violation of the Texas Wiretap Acts, Tex. Code Crim. P. art. 18.20, § 1(3) and Tex. Pen. Code § 16.02(a); violation of the Texas Theft Liability Act, Tex. Pen. Code § 31.03; violation of the federal Computer Fraud & Abuse Act, 18 U.S.C. § 1030; violation of the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2510; and violation of Racketeer Influenced and Corrupt Organizations Act (“RICO”), 18 U.S.C. § 1961–1964. In addition, Plaintiffs assert common law claims for negligent misrepresentation, invasion of privacy (intrusion upon seclusion and public disclosure of private facts), conversion, trespass to personal property and/or chattel, misappropriation, strict product liability (design defect and failure to warn), negligence, and secondary and vicarious liability.³

The following chart shows which claims each Plaintiff asserts against each Defendant:

	Cause of Action	On Behalf of	Against
1	UCL	All Plaintiffs	Apple
2	UCL	Opperman Plaintiffs	Apple
3	UCL	Plaintiffs Except Pirozzi	App Defendants
4	FAL	All Plaintiffs	Apple
5	FAL	Opperman Plaintiffs	Apple
6	CLRA	All Plaintiffs	Apple
7	CLRA	Opperman Plaintiffs	Apple
8	Negligent Misrepresentation	All Plaintiffs	Apple
9	Negligent Misrepresentation	Opperman Plaintiffs	Apple

³ Plaintiffs, Apple, and the App Defendants discuss California and Texas common law interchangeably without explanation, often pointing out that both states’ common law is identical with respect to the issues presented by Defendants’ motions to dismiss. The Court has not identified any differences between Texas and California common law on the issues addressed in this Order, and therefore, for the sake of convenience, discusses only California law.

	Cause of Action	On Behalf of	Against
10	CDAFA	Plaintiffs Except Pirozzi	All Defendants
11	CFAA	Plaintiffs Except Pirozzi	App Defendants
12	ECPA	Plaintiffs Except Pirozzi	App Defendants
13	Wiretap/Invasion of Privacy Act	CAD Plaintiffs ⁴	Foodspotting, Instagram, Path, Twitter, and Yelp
14	Texas Wiretap Acts	Texas Plaintiffs ⁵	App Defendants
15	Intrusion Upon Seclusion	Opperman Plaintiffs	App Defendants
16	Public Disclosure of Private Facts	Opperman Plaintiffs	App Defendants
17	Conversion	Plaintiffs Except Pirozzi	All Defendants
18	Trespass to Property	Opperman Plaintiffs	All Defendants
19	Texas Theft Liability Act	Texas Plaintiffs	App Defendants
20	Misappropriation	Opperman Plaintiffs	App Defendants
21	Strict Products Liability: Design Defect	Opperman Plaintiffs	Apple
22	Strict Products Liability: Failure to Warn	Opperman Plaintiffs	Apple
23	Negligence	Plaintiffs Except Pirozzi	All Defendants
24	Uniform Fraudulent Transfer Act	Gowalla Plaintiffs	Gowalla and Facebook
25	RICO	Opperman Plaintiffs	All Defendants
26	Secondary and Vicarious Liability	Opperman Plaintiffs	All Defendants

The following summary of Plaintiffs' allegations is taken from the complaint. As it must, the Court accepts the CAC's allegations as true for purposes of this motion.

A. The App Store

Apple launched the App Store in 2008, and heavily promoted it in conjunction with its iDevices. CAC ¶ 57. The promotion was successful: the App Store today has over 700,000 apps for iPhone and iPod touch, and 275,000 apps for the iPad. Since 2008, customers have downloaded over forty billion apps. Id.

Apple maintains "exclusive domain" and "ultimate control" over the App Store's

⁴ "CAD" Plaintiffs are those who downloaded apps from Foodspotting, Instagram, Path, Twitter, and Yelp.

⁵ The Texas Plaintiffs are Beuershasen, Biondi, Dean, Hodgins, Hoffman, King, and Varner.

offerings. iDevices are designed only to accept apps from the App Store, and Apple decides which apps will be offered, and which will not. CAC ¶ 60. iDevices also come with pre-programmed apps built into the device's operating system. Among those apps is Apple's "Contacts" app — a virtual address book. The App Store is another one. CAC ¶ 61. Neither of these built-in apps can be removed by the user.

"Apple claims to review each application before offering it to its users, purports to have implemented apps privacy standards, and claims to have created a strong privacy protection for its customers." CAC ¶ 62. However, some apps offered on the App Store are alleged to have accessed and uploaded information from customers' iDevices without their knowledge, including contact information. Plaintiffs allege that Apple has failed to safeguard the App Store from such apps, while representing to the public that Apple's products are "safe and secure." CAC ¶ 64.

Apple is "notorious for complete control over its products." CAC ¶ 87. App developers must submit their apps to Apple for review, and Apple decides whether to offer them on the App Store. To be eligible for inclusion, third-party app developers must register with Apple and agree to the iOS Developer Agreement ("IDA") and the Program License Agreement ("PLA"), as well as pay a yearly registration fee. CAC ¶ 87–89. Apple reserves the right to reject apps for any reason, and has explicitly reserved the right to reject apps that breach the licensing agreements, provide Apple with inaccurate documents or information, or violate, misappropriate, or infringe the rights of a third party. CAC ¶ 90. After joining the program, app developers use Apple's software development kit ("SDK"), which provides guidelines and tools for app development. CAC ¶ 91.

The App Store Review Guidelines prohibit the transmission of user data without prior permission. CAC ¶¶ 101, 104. However, Plaintiffs allege that Apple's "iOS Human Interface Guidelines" encourage data theft. The guidelines are meant to guide developers as they create apps for the App Store. Apple tells developers, "don't force people to give you information you can easily find for yourself, such as their contacts or calendar information," and "[i]f possible, avoid requiring users to indicate their agreement to your [end user license agreement] when they first start your application. Without an agreement displayed, users can enjoy your application

1 without delay.” CAC ¶ 212 (emphasis omitted).

2 Plaintiffs allege that “Apple taught Program registrants’ to incorporate forbidden data
3 harvesting functionalities — even for private “contacts” — into their Apps and encouraged
4 Program registrants to design those functions to operate in non-discernible manners that would not
5 be noticed by the iDevice owner. These App Defendants, apparently in accord with Apple’s
6 instructions, did just that with their identified Apps.” CAC ¶ 214.

7 Similarly, Plaintiffs allege: “Apple’s Program tutorials and developer sites [] teach
8 Program registrants how to code and build apps that non-consensually access, manipulate, alter,
9 use and upload the mobile address books maintained on Apple iDevices.” CAC ¶ 190.

10 **B. The Subject Apps**

11 Plaintiffs allege that each of the App Defendants developed an app that copied iDevice
12 users’ contact information without the user’s consent. In February 2012, it was revealed that App
13 Defendant Path’s app, also called “*Path*,” was uploading users’ contacts and calendar information
14 to its servers without users’ knowledge. Path’s CEO publicly apologized after the practice was
15 made public. CAC ¶ 110.

16 Plaintiffs allege that several popular apps, including those designed by each App
17 Defendant, have accessed and uploaded user data without consent. In some of these cases, the
18 apps accessed user data without any prompt at all. See CAC ¶¶ 112, 136. *Path* is one such app.
19 In other cases, the apps “surreptitiously accessed and uploaded information from users’ Contacts
20 app through a ‘Find Friends’ feature without disclosing to users that the feature would leave their
21 private information vulnerable to unauthorized download by the third-party app manufacturer.”
22 CAC ¶ 108.

23 The public revelations concerning third parties’ access to users’ private information led
24 Congressmen Waxman and Butterfield to write to Apple and to thirty-four app publishers in
25 February and March of 2012, asking for more information about the practice. CAC ¶¶ 115–17

26 The February letter to Apple noted that Apple’s website at that time represented that
27 iDevice apps “have access to a device’s global data such as contacts in the Address Book,” while
28 Apple’s review guidelines required app developers to gain users’ permission prior to transmitting

data about a user. CAC ¶ 115. The letter continues:

In spite of this guidance, claims have been made that “there’s a quiet understanding among many iOS app developers that it is acceptable to send a user’s entire address book, without their permission, to remote servers and then store it for future reference. It’s common practice, and many companies likely have your address book stored in their database.” One blogger claims to have conducted a survey of developers of popular iOS apps and found that 13 of 15 had a “contacts database with millions of records” — with one claiming to have a database containing “Mark Zuckerberg’s cell phone number, Larry Ellison’s home phone number and Bill Gates’ cell phone number.

Id. In March 2012, Senator Schumer called for an investigation by the Federal Trade Commission. CAC ¶ 118. In September 2012, Apple released iOS 6, which updated privacy settings on iDevices in a manner that discloses which apps access users’ contacts, calendars, reminders, photos, and other personal information, and allows users a way to prevent certain apps from accessing certain information. CAC ¶ 120.

The following chart outlines the apps each Plaintiff alleges he or she downloaded and deployed:

Plaintiff	Angry Birds	Angry Birds Classic	Cut The Rope	Foodspotting	Foursquare	Gowalla	Hipster	Instagram	Kik Messenger	Path	Twitter	Yelp!
Alan Beuershasen		X			X	X					X	
Giuli Biondi			X					X			X	X
Lauren Carter										X		
Steve Dean		X				X					X	
Stephanie Dennis-Cooley								X	X	X	X	
Jason Green		X	X					X	X	X	X	
Claire Hodgins		X	X								X	X
Gentry Hoffman					X			X			X	X
Rachelle King				X	X	X	X	X			X	
Nirali Mandaywala		X	X		X	X		X			X	X
Claire Moses								X			X	
Judy Paul					X	X				X	X	X
Maria Pirozzi	X											
Theda Sandiford		X	X	X	X	X		X			X	
Greg Varner		X	X		X	X		X			X	

C. Apple's Representations

Plaintiffs allege that “Apple has repeatedly represented that Apple’s products are safe and secure, and that private information could not be accessed by third-party apps without the user’s express consent.” CAC ¶ 64. Throughout the CAC, Plaintiffs identify representations Apple has made on its website, in in-store advertisements, and otherwise, to the effect that iOS is “highly secure,” sometimes in particular with respect to the accessing of data by apps from other apps. See CAC ¶¶ 102–04, 121–123.

For example, when the App Store first launched, Apple’s former CEO Steve Jobs explained, “[t]here are going to be some apps that we’re not going to distribute. Porn, malicious apps, apps that invade your privacy.” CAC ¶ 92. Plaintiffs allege that Apple repeated this refrain continuously during the launch of the App Store, and publicly took action consistent with these goals. See CAC ¶¶ 93–98. In October 2007, Jobs stated: “It will take until February to release an SDK because we’re trying to do two diametrically opposed things at once — provide an advanced and open platform to developers while at the same time protect iPhone users from viruses, malware, privacy attacks, etc. As our phones become more powerful, these malicious programs will become more dangerous.” CAC ¶ 94. At an SDK press conference on March 6, 2008, Jobs repeated that Apple would place limitations on third party apps for “malicious” and “illegal” content in order to address “privacy” concerns. CAC ¶ 93. Apple also “famously refused to integrate Adobe Flash technology” despite user demands. Jobs explained in April 2010 that this decision was made “because of reliability, security, and performance concerns.” CAC ¶ 97. “In sum, Apple has attempted to cultivate a perception that its products are safe and that Apple strives to protect users.” CAC ¶ 99.

In September 2011, Apple’s website stated that “iOS 4 is highly secure from the moment you turn on your iPhone. All apps run in a safe environment, so a website or app can’t access data from other apps.” CAC ¶ 102. Apple also assured consumers that, for data-security purposes, “Applications on the device are ‘sandboxed’ so they cannot access data stored by other applications.” CAC ¶ 209.

Apple’s “customer privacy policy” states that Apple takes “precautions — including

administrative, technical, and physical measures — to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction.” CAC ¶ 122.

Plaintiffs further allege that “[f]rom 2008 to the present, the highest levels of Apple (from its founder to its current CEO to its corporate spokespersons) have so consistently expressed publicly that Apple protects its customers’ and iDevice owners’ security and privacy that — though inaccurate — it is ingrained into the image of Apple’s culture, products and offerings as well as in the minds of customers.” CAC ¶ 211.

Plaintiffs allege they saw and relied on Apple’s website, in-store advertisements, and television advertising in purchasing their iDevices, and that they would have paid less for their devices, or not purchased them at all, had they known they were vulnerable to privacy attacks. See CAC ¶ 125–26.

II. LEGAL STANDARDS

On a motion to dismiss, the Court accepts the material facts alleged in the complaint, together with all reasonable inferences to be drawn from those facts, as true. Navarro v. Block, 250 F.3d 729, 732 (9th Cir. 2001). However, “the tenet that a court must accept a complaint’s allegations as true is inapplicable to threadbare recitals of a cause of action’s elements, supported by mere conclusory statements.” Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). To be entitled to the presumption of truth, a complaint’s allegations “must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively.” Starr v. Baca, 652 F.3d 1202, 1216 (9th Cir. 2011), cert. den’d, --- U.S. ----, 132 S.Ct. 2101 (2012).

To survive a motion to dismiss, a plaintiff must plead “enough facts to state a claim to relief that is plausible on its face.” Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 570 (2007). Plausibility does not mean probability, but it requires “more than a sheer possibility that a defendant has acted unlawfully.” Iqbal, 556 U.S. at 687. “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* In the Ninth Circuit, “[i]f there are two

1 alternative explanations, one advanced by defendant and the other advanced by plaintiff, both of
2 which are plausible, plaintiff's complaint survives a motion to dismiss under Rule 12(b)(6).
3 Plaintiff's complaint may be dismissed only when defendant's plausible alternative explanation is
4 so convincing that plaintiff's explanation is implausible." Starr, 652 F.3d at 1216 (original
5 emphasis).

6 In addition, fraud claims are subject to a heightened pleading standard. "In alleging fraud
7 or mistake, a party must state with particularity the circumstances constituting fraud or mistake."
8 Fed. R. Civ. P. 9(b). The allegations must be specific enough to give a defendant notice of the
9 particular misconduct alleged to constitute the fraud such that the defendant may defend against
10 the charge. Semegen v. Weidner, 780 F.2d 727, 731 (9th Cir. 1985). In general, allegations
11 sounding in fraud must contain "an account of the time, place, and specific content of the false
12 representations as well as the identities of the parties to the misrepresentations." Swartz v. KPMG
13 LLP, 476 F.3d 756, 765 (9th Cir. 2007). However, "[m]alice, intent, knowledge, and other
14 conditions of a person's mind may be alleged generally." Fed. R. Civ. P. 9(b).

15 Finally, a "Rule 12(b)(1) jurisdictional attack may be facial or factual. In a facial attack,
16 the challenger asserts that the allegations contained in a complaint are insufficient on their face to
17 invoke federal jurisdiction. By contrast, in a factual attack, the challenger disputes the truth of the
18 allegations that, by themselves, would otherwise invoke federal jurisdiction." Safe Air for
19 Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004) (citation omitted). In resolving a facial
20 attack, courts assume that the allegations are true, and draw all reasonable inferences in the
21 plaintiff's favor. Wolfe v. Strankman, 392 F.3d 358, 362 (9th Cir. 2004) (citations omitted). "In
22 resolving a factual attack on jurisdiction, the district court may review evidence beyond the
23 complaint without converting the motion to dismiss into a motion for summary judgment. The
24 court need not presume the truthfulness of the plaintiff's allegations. Once the moving party has
25 converted the motion to dismiss into a factual motion by presenting affidavits or other evidence
26 properly brought before the court, the party opposing the motion must furnish affidavits or other
27 evidence necessary to satisfy its burden of establishing subject matter jurisdiction." Safe Air, 373
28 F.3d at 1039 (citations omitted).

III. APPLE'S MOTION TO DISMISS

Apple moves to dismiss all of Plaintiffs' claims on Article III standing grounds, as well as each of Plaintiffs' substantive claims for failure to state a claim upon which relief can be granted. Because Article III standing is a threshold jurisdictional question, the Court will first address Apple's Rule 12(b)(1) motion to dismiss on the grounds that Plaintiffs lack Article III standing. See Steel Co. v. Citizens for a Better Env., 523 U.S. 83, 94 (1998).

A. Article III Standing

1. Legal Standards

To establish Article III standing, a plaintiff in federal court must meet three requirements. First, the plaintiff must have suffered an "injury in fact" — an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct complained of — the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court. Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992).

The standing requirements are not pleading requirements. Rather, "each element must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation." Id. at 561. Nevertheless, "[a]t the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice." Id. A "court's obligation to take a plaintiff at its word at that stage in connection with Article III standing issues is primarily directed at the injury in fact and causation issues, not redressability." Levine v. Vilsack, 587 F.3d 986, 996–97 (9th Cir. 2009) (citing Lujan, 504 U.S. at 561). "[I]t is within the trial court's power to allow or to require the plaintiff to supply, by amendment to the complaint or by affidavits, further particularized allegations of fact deemed supportive of plaintiff's standing." Warth v. Seldin, 422 U.S. 490, 501–02 (1975).

In addition, even when a plaintiff is able to establish Article III standing, prudential

considerations may preclude the exercise of federal jurisdiction. A plaintiff's claim must fall within the "zone of interests" sought to be protected by the statute or constitutional provision in question. Bond v. United States, ___ U.S. ___, 131 S. Ct. 2355, 2366–67 (2011). That claim must be based on the plaintiff's own legal rights and interests rather than the legal rights or interests of third parties. Elk Grove Unified School Dist. v. Newdow, 542 US 1, 15 n.7 (2004). And the injury must be individualized, or confined to a discrete group; courts will not adjudicate "abstract questions of wide public significance" amounting only to "generalized grievances." Valley Forge Christian College v. Americans United for Separation of Church & State, Inc., 454 U.S. 464, 474–75 (1982) (quoting Warth, 422 U.S. at 499–50).

Finally, in a class action, it is not sufficient for any named plaintiff to rely on the injuries suffered by the class to satisfy Article III standing requirements; each named plaintiff must meet the standing requirements, including satisfactorily alleging that each named plaintiff suffered "non-speculative injury." Lierboe v. State Farm Mut. Auto. Ins. Co., 350 F.3d 1018, 1022 (9th Cir. 2003).

2. Injury-in-Fact and Causation

Despite the presence of fifteen named Plaintiffs and fifteen Defendants, and the assertion of twenty-six causes of action, Plaintiffs' case is rather simple. Plaintiffs allege that Apple sold them devices that made it possible for third parties to access and copy Plaintiffs' address books without their knowledge. Plaintiffs allege, with respect to Apple, that they suffered injury in the form of having overpaid for their iDevices, because they would have paid less for their devices, or not purchased them at all, if Apple had disclosed that it had failed adequately to secure the devices from the alleged intrusion.

In denying Apple's second motion to dismiss Plaintiff Pirozzi's⁶ claims on standing grounds, this Court observed that her alleged overpayment injury satisfied Article III's injury-in-fact requirement because "palpable economic injuries have long been recognized as sufficient to lay the basis for standing." Sierra Club v. Morton, 405 U.S. 727, 733–34 (1972); see also Comm.

⁶ Pirozzi's action was related to the above-captioned action, and her claims are now grouped in the CAC with the claims of the other fourteen Plaintiffs.

v. Reno, 98 F.3d 1121, 1130 (9th Cir. 1996) (“Economic injury is clearly a sufficient basis for standing.”). See Pirozzi v. Apple, Inc., No. 12-cv-01529-JST, ___ F. Supp. 2d ___, 2013 WL 4029067, at *4 (N.D. Cal. Aug. 5, 2013) (“Pirozzi II”). Judge Gonzalez Rogers previously reached the same conclusion. See Pirozzi v. Apple, Inc., No. 12-cv-1529-YGR, 913 F. Supp. 2d 840, 847 (N.D. Cal. Dec. 20, 2012) (“Pirozzi I”) (“Apple’s arguments misconstrue the nature of Plaintiff’s allegations Overpaying for goods or purchasing goods a person otherwise would not have purchased based upon alleged misrepresentations by the manufacturer would satisfy the injury-in-fact and causation requirements for Article III standing.”).

Nevertheless, Apple argues that Plaintiffs have not satisfied the causation requirement because no Plaintiff has identified the specific representations made by Apple that form the basis of their overpayment theory of liability. The CAC makes the following allegations concerning Apple’s alleged misrepresentations and Plaintiffs’ reliance:

[E]ach Plaintiff viewed Apple’s online, in-store, and/or television advertisements. In addition, each Plaintiff relied on Apple’s reputation for safety, cultivated through Apple’s extensive marketing and advertising campaigns. Each Plaintiff purchased an iDevice with the expectation that (i) it would come with a fully functioning App Store, and (ii) that Plaintiff would be able to utilize the “Contacts” function and iDevice apps from the App Store without compromising the security, safety, or control of Plaintiff’s iDevice, mobile address book, or other personal and private information. Indeed, each Plaintiff purchased an iDevice with the expectation that he or she would maintain a mobile address book and receive and use additional add-on apps on his or her iDevice. Had any Plaintiff known that iDevices lacked promised features or that Apple designed the iDevices with known vulnerabilities to unauthorized operations from Apple-issued [third-party] apps, Plaintiffs would not have accepted add-on apps from Apple or the App Store and would have paid less for his or her iDevice. At no time prior to the purchase of Plaintiffs’ iDevice did Apple warn any Plaintiff that the iDevice and its data — particularly the Contacts feature and mobile address book — were vulnerable to unauthorized control and dissemination by third-parties.

CAC ¶ 32.

Apple’s standing argument fails to appreciate that “the threshold question of whether plaintiff has standing (and the court has jurisdiction) is distinct from the merits of his claim.

1 Rather, “[t]he jurisdictional question of standing precedes, and does not require, analysis of the
 2 merits.” Maya v. Centex Corp., 658 F.3d 1060, 1068 (9th Cir. 2011) (quoting Equity Lifestyle
 3 Props., Inc. v. Cnty. of San Luis Obispo, 548 F.3d 1184, 1189 n.10 (9th Cir. 2008)). In other
 4 words, it is possible that Plaintiffs may file a civil action “without suffering dismissal for want of
 5 standing to sue,” even though they are “[un]able to assert a cause of action successfully.”⁷ In re
 6 Facebook Privacy Litig., 791 F. Supp. 2d 705, 712 n.5 (N.D. Cal. 2011) (quoting Doe v. Chao,
 7 540 U.S. 614, 624–25 (2004)). See also Warth, 422 U.S. at 500 (standing “in no way depends on
 8 the merits of the [] contention that particular conduct is illegal.”); Catholic League for Religious
 9 and Civil Rights v. City & Cnty. of San Francisco, 624 F.3d 1043, 1049 (9th Cir. 2010) (en banc)
 10 (standing analysis may not “be used to disguise merits analysis, which determines whether a claim
 11 is one for which relief can be granted if factually true.”).

12 For the Court to have jurisdiction over Plaintiffs’ claims, their alleged injury must be
 13 “fairly traceable” to Apple, and not the result of the “independent action of some third party not
 14 before the court.” Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992) (quoting Simon
 15 v. Eastern Ky. Welfare Rights Organization, 426 U.S. 26, 41–42 (1976)). Plaintiffs’ claims meet
 16 that requirement: Plaintiffs allege that Apple misled them through its advertising and failed to
 17 disclose material information, that each Plaintiff relied on these misrepresentations or non-
 18 disclosures, and that each Plaintiff overpaid for Apple’s products. The requirements to allege
 19 standing are not the same as the requirements to plead injury under the substantive law. See Low
 20 v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1027 (N.D. Cal. 2012) (holding plaintiffs satisfied
 21 Article III standing even though they had failed to allege reliance on particular representations,
 22

23 ⁷ Apple’s reliance on In re iPhone Application Litig. (“iPhone III”), No. 11-md-2250-LHK, ___ F.
 24 Supp. 2d ___, 2013 WL 6212591, at *8 (N.D. Cal. Nov. 25, 2013), underlines the importance of
 25 accounting for the stage of litigation at which the Court engages in the standing analysis. After
 26 sustaining the plaintiffs’ claims and finding they did not lack standing at the pleading stage, the
 27 court in iPhone III granted summary judgment on standing grounds because Apple adduced
 28 “specific facts” through discovery that established a lack of evidence of causation, fatally
 undermining the plaintiffs’ Article III standing. Here, Plaintiffs’ allegations are, at the pleading
 stage, sufficient to establish standing. That development of the factual record *may* one day dictate
 a different result does not alter the Court’s analysis now.

and even though their FAL claims were dismissed with prejudice on that basis).⁸

Plaintiffs are also independently able to establish standing through their statutory claims because “[t]he injury required by Article III can exist solely by virtue of ‘statutes creating legal rights, the invasion of which creates standing.’” Edwards v. First Am. Corp., 610 F.3d 514, 517 (9th Cir. 2010) (quoting Fulfillment Servs. Inc. v. United Parcel Serv., Inc., 528 F.3d 614, 618 (9th Cir. 2008)). See also Robins v. Spokeo, Inc., No. 11-56843, ___ F.3d ___, 2014 WL 407366, at *2–3 (9th Cir. Feb. 4, 2014) (“[T]he violation of a statutory right is usually a sufficient injury in fact to confer standing.”). “The scope of the cause of action determines the scope of the implied statutory right When, as here, the statutory cause of action does not require proof of actual damages, a plaintiff can suffer a violation of the statutory right without suffering actual damages.” Id. (citation omitted). Apple does not respond to this argument, other than to argue that Plaintiffs cannot establish those substantive claims.

Apple makes several more arguments concerning the merits of Plaintiffs’ claims, including that Plaintiffs have failed to allege their address books were actually uploaded,⁹ and that Apple is not responsible for the App Defendants’ conduct. None of these arguments affect the Court’s standing analysis and are better left to the question of whether Plaintiffs have failed to state a claim upon which relief can be granted.

⁸ There is further support in the CAC for Plaintiffs’ standing. Plaintiffs allege that Apple contributed to the theft of address books through its review of App Store submissions, its App Store review guidelines, its software development kit, other sources of guidance Apple makes available to app developers, and through its failure to catch the offending features contained in the apps implicated in this suit. Plaintiffs also assert product liability claims against Apple for its design of iDevices, and for its failure to warn consumers of their alleged defects. Again, the Court notes that the question of whether these allegations suffice to establish any of Plaintiffs’ claims against Apple is separate from the question of whether these allegations are sufficient to invoke the Court’s subject matter jurisdiction.

⁹ In fact, the CAC alleges that apps designed by each App Defendant were downloaded by at least one Plaintiff, and that each of those apps has been shown to upload users’ address books without consent after a known set of steps is taken by the user. That Plaintiffs do not allege that their information was, in fact, uploaded is not surprising, since only discovery will reveal whether and how the allegedly widespread practice affected each Plaintiff. But Plaintiffs plausibly allege that they “unwittingly took those steps . . . needed to unwittingly trigger the unnoticeable transmission of their mobile address books.” CAC ¶ 139.

1 Finally, relying on In re LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089, 1094 (N.D.
2 Cal. 2013), Apple argues that an overpayment claim cannot survive without an allegation of
3 “something more” than overpaying for a defective product, such as an allegation that the address
4 books were actually stolen. In LinkedIn, the court held that, “in cases where the alleged wrong
5 stems from allegations about insufficient performance or how a product functions, courts have
6 required plaintiffs to allege ‘something more’ than ‘overpaying for a “defective” product.’” In re
7 LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013) (citing In re Toyota
8 Motor Corp., 790 F.Supp.2d 1152, 1165 n. 11 (C.D.Cal.2011)).

9 Apple misreads LinkedIn and the cases upon which the LinkedIn court relied. The
10 deficiency in the LinkedIn plaintiffs’ standing was that they were pleading only a difference
11 between what they had been promised by LinkedIn and what they had received, *i.e.*, a breach of
12 contract. In re LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013)
13 (“Plaintiffs cannot rely solely on the ‘benefit of the bargain’ theory of economic harm to
14 sufficiently meet the requirements for Article III standing”). They did not allege that they had
15 suffered any other separate injury.

16 More relevant here is the decision in In re Toyota Motor Corp., 790 F. Supp. 2d 1152,
17 1165 (C.D. Cal. 2011), on which the LinkedIn court relied. There, the plaintiffs alleged that they
18 relied on Toyota’s “advertisements for Toyota vehicles on television, in magazines, on billboards,
19 in brochures at the dealership, on the Internet, in newspapers, and on banners in front of the
20 dealership,” throughout which “safety and reliability” were a “consistent theme.” Id. at 1161. The
21 plaintiffs also alleged that, had Toyota disclosed the safety defect in its vehicles of which they
22 complained, they would not have purchased their vehicles, or would have paid less for them.
23 Relatedly, they alleged that their vehicles were worth less in the used car market as a consequence
24 of the public revelations concerning the safety defect. The Toyota Motors court rejected many of
25 the same standing arguments Apple advances here because “once the safety defect is sufficiently
26 and plausibly pled by all Plaintiffs, the economic losses resulting from the defect are readily
27 established: defective cars are simply not worth as much.” Id. at 1163. This was so even though
28 the defect had not manifested in all of the plaintiffs’ vehicles. As the Toyota Motors court

1 explained,

2 When the economic loss is predicated solely on how a product
3 functions, and the product has not malfunctioned, the Court agrees
4 that something more is required than simply alleging an
5 overpayment for a “defective” product [T]hat “something
6 more” could be allegations based on market forces. It could also be
7 based on sufficiently detailed, non-conclusory allegations of the
8 product defect.

9 Id. at 1165 n.11.

10 Here, the Court finds that Plaintiffs’ allegations concerning the offending feature of the
11 product — design that enables third parties to take address book information without consent —
12 supply the “something more” that is required. Whether Plaintiffs’ product liability claims state a
13 claim upon which relief can be granted is a separate question the Court addresses below.

14 Separately, Plaintiffs allege injury-in-fact to their property rights in their address books, as
15 distinct from the economic injury of overpayment for their iDevices, as support for their common
16 law conversion and trespass claims. The Court discusses this allegation in connection with the
17 App Defendants’ motion to dismiss in more detail *infra*, Part IV.A. For the reasons discussed in
18 that section, the Court finds that Plaintiffs lack Article III standing based on any injury to their
19 property rights in their address books. For this reason, the Court will dismiss Plaintiffs’ common
20 law claims against Apple for conversion and trespass.

21 **3. Non-Resident Plaintiffs**

22 Apple also argues that the non-resident Plaintiffs lack standing to assert California
23 statutory claims. That argument “conflate[s] two issues: the extraterritorial application of
24 California consumer protection laws (or the ability of a nonresident plaintiff to assert a claim
25 under California law), and choice-of-law analysis” Forcellati v. Hyland’s, Inc., 876 F. Supp.
26 2d 1155, 1160 (C.D. Cal. 2012). “Whether a nonresident plaintiff can assert a claim under
27 California law is a constitutional question based on whether California has sufficiently significant
28 contacts with the plaintiff’s claims.” Id. (citing Mazza v. American Honda Motor Co., 666 F.3d
581, 589 (9th Cir. 2012)). In Mazza, for example, “California ha[d] a constitutionally sufficient
aggregation of contacts to the claims of each putative class member . . . because Honda’s corporate
headquarters, the advertising agency that produced the allegedly fraudulent misrepresentations,

1 and one fifth of the proposed class members [were] located in California.” Mazza, 666 F.3d at
 2 589. In Forcellati, the fact that the defendant was alleged to be headquartered in Los Angeles led
 3 the court to conclude that “application of California law poses no constitutional concerns.”
 4 Forcellati, 876 F. Supp. 2d at 1160.

5 Apple’s arguments here were recently rejected by Judge Wilken in another case arising out
 6 of Apple’s marketing activities. See In re iPhone 4S Consumer Litig., No. 12-cv-1127-CW, 2013
 7 WL 3829653, at *7–8 (N.D. Cal. July 23, 2013). There, the plaintiffs “alleged that their injuries
 8 were caused by Apple’s wrongful conduct in false advertising that originated in California.” Id. at
 9 *7. Judge Wilken noted that the presumption against the extraterritoriality of California law does
 10 not apply where the misconduct occurs in California. See Wershba v. Apple Computer, Inc., 91
 11 Cal. App. 4th 224, 243 (2001) (California statutes apply to “non-California members of a
 12 nationwide class where the defendant is a California corporation and some or all of the challenged
 13 conduct emanates from California.”). Judge Wilken also distinguished In re Apple & AT&T iPad
 14 Unlimited Data Plan Litig., 802 F. Supp. 2d 1070, 1076 (N.D. Cal. 2011), upon which Apple also
 15 relies here, because in that case, unlike here, a contractual choice-of-law clause selected the law of
 16 each customer’s state of residence. The Court agrees with Judge Wilken’s careful analysis in the
 17 iPhone 4S decision.

18 Apple relies heavily on Sullivan v. Oracle Corp., 51 Cal. 4th 1191, 1209 (2011), for
 19 support. Sullivan concerned an overtime claim asserted under the unlawful prong of the UCL, the
 20 predicate offense for which was a violation of the federal Fair Labor Standards Act (“FLSA”).¹⁰
 21 The plaintiffs alleged that the employer had made the decision to mis-classify workers in
 22 California. Noting that “the UCL reaches any unlawful business act or practice committed in
 23 California,” the court found that “for an employer to adopt an erroneous classification policy is not
 24 unlawful in the abstract.” Id. at 1208. Consequently, the court held that the UCL “does not apply
 25 to overtime work performed outside California for a California-based employer by out-of-state
 26 plaintiffs in the circumstances of this case based solely on the employer’s failure to comply with
 27

28 ¹⁰ The Ninth Circuit had certified the question for the California Supreme Court to answer.

the overtime provisions of the FLSA.” Id. Thus, the California Supreme Court’s holding (1) did not undermine the established presumption that nonresident plaintiffs may assert California claims to address unlawful conduct committed in California by a California resident; and (2) was limited to the FLSA overtime pay context because the work is “performed outside California.” Other courts have come to the conclusion, as this Court does, that Sullivan provides no support for the argument that a national class cannot assert California fraud claims against a California corporation for its misleading marketing. See, e.g., Gross v. Symantec Corp., No. 12-cv-154-CRB, 2012 WL 3116158, at *7 n.10 (N.D. Cal. July 31, 2012); Parkinson v. Hyundai Motor America, 258 F.R.D. 580, 598 (C.D. Cal. 2008).

The Court notes that Apple has not argued that the Court should apply the law of each plaintiff’s home state to her claims, and the Court does not reach the question of whether it should. The Court only concludes that it is constitutional for the nonresident Plaintiffs to assert California statutory claims against Apple based on Apple’s conduct in California. For this reason, Apple’s reliance on the choice-of-law analysis in In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942 (S.D. Cal. 2012), and Frezza v. Google, Inc., No. 12-cv-237-RMW, 2013 WL 1736788, at *5 (N.D. Cal. Apr. 22, 2013), is misplaced. The question of whether the CAC presents a certifiable class under Mazza, and in particular, how a choice-of-law analysis would affect class certification, is a question for another day.

B. Communications Decency Act

Apple moves to dismiss all of Plaintiffs’ claims against it, except those premised on Apple’s alleged misrepresentations, on the ground that the Communications Decency Act (“CDA”), 47 U.S.C. § 230, bars Plaintiffs’ claims. Section 230(c)(1) provides: “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” Section 230(c)(2) provides:

No provider or user of an interactive computer service shall be held liable on account of--

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or

otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in [section 230(c)(1)].

Pursuant to the Act, an “interactive computer service” is “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.” 47 U.S.C. § 230(f)(2). An “information content provider” is “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.” 47 U.S.C. § 230(f)(3).

Congress enacted these provisions as part of the Communications Decency Act of 1996 “for two basic policy reasons: to promote the free exchange of information and ideas over the Internet and to encourage voluntary monitoring for offensive or obscene material. Carafano v. Metroplash.com, Inc., 339 F.3d 1119, 1122 (9th Cir. 2003). “In light of these concerns, reviewing courts have treated § 230(c) immunity as quite robust, adopting a relatively expansive definition of ‘interactive computer service’ and a relatively restrictive definition of ‘information content provider.’ Under the statutory scheme, an ‘interactive computer service’ qualifies for immunity so long as it does not also function as an ‘information content provider’ for the portion of the statement or publication at issue.” Id. at 1123 (footnotes omitted).

Nevertheless, neither section 230(c) nor any other subsection in the CDA “declares a general immunity from liability deriving from third-party content.” Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100 (9th Cir. 2009). Instead, to determine whether the CDA operates as a bar to civil liability, courts must determine whether “a plaintiff’s theory of liability would treat a defendant as a publisher or speaker of third-party content.” Id. at 1101. “[W]hat matters is not the name of the cause of action — defamation versus negligence versus intentional infliction of emotional distress — what matters is whether the cause of action inherently requires the court to treat the defendant as the ‘publisher or speaker’ of content provided by another. To put it another way, courts must

ask whether the duty that the plaintiff alleges the defendant violated derives from the defendant's status or conduct as a 'publisher or speaker.' If it does, section 230(c)(1) precludes liability." Id. at 1101–02.

Determining whether a defendant is a "publisher" requires further definition of that term. The Ninth Circuit has held that "publication involves reviewing, editing, and deciding whether to publish or to withdraw from publication third-party content." Id. at 1102. "[A] publisher reviews material submitted for publication, perhaps edits it for style or technical fluency, and then decides whether to publish it." Id. Despite Plaintiffs' arguments to the contrary,¹¹ "it is immaterial whether this decision comes in the form of deciding what to publish in the first place or what to remove among the published material. This is particularly so in the context of the internet, where material can be 'posted' and 'unposted' with ease." Id. at 1102 n.8 (citing Batzel v. Smith, 333 F.3d 1018, 1032 (9th Cir. 2003)). Cf. Batzel v. Smith, 333 F.3d 1018, 1032 (9th Cir. 2003) ("A distinction between removing an item once it has appeared on the Internet and screening before publication cannot fly [].").

By contrast, the CDA does not bar claims against "information content providers." An entity "that is responsible, in whole or in part, for the creation or development" of the allegedly offending information is not entitled to the CDA's protection. "Development" refers "not merely to augmenting the content generally, but to materially contributing to its alleged unlawfulness." Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1167–68 (9th Cir. 2008). Thus, "providing *neutral* tools to carry out what may be unlawful or illicit searches does not amount to 'development' for purposes of the immunity exception." Id. at 1169. Nor does inoffensive editing for spelling errors, removing obscenity, or trimming for length. However, "a website operator who edits in a manner that contributes to the alleged illegality — such as by removing the word 'not' from a user's message reading '[Name] did *not* steal the artwork' in order to transform an innocent message into a libelous one — is directly involved in the alleged illegality and thus not immune." Id.

¹¹ Plaintiffs argue that the CDA protects only an interactive computer service's decision to exclude offensive content.

Prior to the relation of Plaintiff Pirozzi's action against Apple to the above-captioned Opperman action, Apple moved to dismiss Pirozzi's claims pursuant to the same provisions of the CDA. Judge Gonzalez Rogers denied Apple's motion on two bases. First, she found that Pirozzi's fraud and misrepresentation claims against Apple arising out of Apple's conduct or failure to disclose were "not predicated *solely* upon Apple's approving and distributing Apps via its online App Store." Pirozzi v. Apple Inc., 913 F. Supp. 2d 840, 849 (N.D. Cal. 2012). Thus, the CDA did not bar those claims. Second, the court held that it was premature to consider the application of the CDA at the pleading stage based on the "scant record" then before the court because "if Apple is responsible for the 'creation or development of [the] information' at issue, then Apple functions as an 'information content provider' *unprotected* by the CDA." Id.

Here, Apple expressly excludes from its CDA argument any application to Plaintiffs' fraud and misrepresentation claims, in recognition of Judge Gonzalez Rogers' first conclusion. With respect to her second conclusion, Apple argues that the CAC, which reproduces many of the allegations in Pirozzi and supplements them with others, contains sufficient allegations from which the Court can now conclude that the CDA bars the remainder of Plaintiffs' claims against Apple. Plaintiffs again maintain that resolution of the CDA issue must await a later stage of the case.

The cases do not describe a one-size-fits all rule for when to apply the CDA. In some cases the applicability of the CDA is "apparent from the face of the complaint"; in others, it is not. Evans v. Hewlett-Packard Co., No. 13-cv-02477-WHA, 2013 WL 5594717, at *3 (N.D. Cal. Oct. 10, 2013) (quoting Goddard v. Google, Inc., 640 F. Supp. 2d 1193, 1200 n.5 (N.D. Cal. 2009)). Here, the Court need not await further discovery before addressing Apple's CDA argument, because the CAC already pleads sufficient conduct to classify Apple as an "information content provider" whose conduct is not protected by the CDA.

For example, Plaintiffs allege that Apple's "iOS Human Interface Guidelines" encourage data theft. The guidelines are meant to guide developers as they create apps for the App Store. Among the guidelines are several suggestions that do, on their face, appear to encourage the practices Plaintiffs complain of in this case. For example, Apple tells developers, "don't force

people to give you information you can easily find for yourself, such as their contacts or calendar information,” and “[i]f possible, avoid requiring users to indicate their agreement to your [end user license agreement] when they first start your application. Without an agreement displayed, users can enjoy your application without delay.” CAC ¶ 212 (emphasis omitted). Based on these passages from the guidelines, Plaintiffs allege: “Apple taught Program registrants’ to incorporate forbidden data harvesting functionalities — even for private “contacts” — into their Apps and encouraged Program registrants to design those functions to operate in non-discernible manners that would not be noticed by the iDevice owner. These App Defendants, apparently in accord with Apple’s instructions, did just that with their identified Apps.” CAC ¶ 214. Similarly, Plaintiffs allege: “Apple’s Program tutorials and developer sites [] teach Program registrants how to code and build apps that non-consensually access, manipulate, alter, use and upload the mobile address books maintained on Apple iDevices.” CAC ¶ 190.

These allegations target conduct that goes beyond the traditional editorial functions of a publisher, and beyond providing “neutral tools to carry out what may be unlawful or illicit” conduct.¹² Apple’s alleged conduct potentially constitutes contribution to the alleged illegality in

¹² It is worth noting that not all of Plaintiffs’ allegations concerning Apple’s conduct fall outside the CDA. For example, Plaintiffs’ assertion that Apple “provides third-party developers with review guidelines, and conducts a review of all applications submitted for inclusion in the App Store for compliance with these documents,” CAC ¶ 89, is identical to an allegation regarding the app distributor in Evans, which that court found insufficient to support the plaintiff’s claim that the distributor was also a co-creator. See Evans, 2013 WL 5594717, at *4 (“plaintiffs allege that defendants ‘[m]andated specific “Application Content Criteria” for all content of the App,’ ‘[m]andated “App Naming Guidelines” for the App,’ and ‘[m]andated technical criteria for the App’”).

Apple’s role as an app publisher, including its promulgation of review guidelines, its review of all apps submitted to the App Store, and its enforcement of its guidelines, is fundamental “publisher” activity protected by the CDA. Plaintiffs’ allegations that Apple has failed to remove offending apps from the App Store, CAC ¶ 90, and that it encourages consumers to download third-party apps and advertises third-party apps in order to sell its devices are similarly subject to the CDA’s protections.

Plaintiffs’ allegations concerning the software development kit also fall under the CDA, because the kit is alleged to be nothing more than a “neutral tool” which app developers can use either lawfully or unlawfully. Nothing in the CAC suggests that the kit itself contributes to the practice of taking contact databases without consent. The kit, technologically speaking, makes that

a manner that invokes the “information content provider” exception to the CDA’s protections. See Roommates.Com, 521 F.3d at 1167–68. At this juncture, the Court therefore cannot conclude that Plaintiffs’ theories of liability deriving from Apple’s encouragement of the harvesting of contact information without obtaining consent from the user are not barred by the CDA. See, e.g., Swift v. Zynga Game Network, Inc., No. 09-cv-05443-SBA, 2010 WL 4569889, at *4–6 (N.D. Cal. Nov. 3, 2010) (allegation that video game developer encouraged the creation of and consumption of special offer “scams” were sufficient at pleading stage).

C. Misrepresentation Claims

Apple groups as “misrepresentation claims” Plaintiffs’ UCL, FAL, CLRA, and negligent misrepresentation claims. Apple argues that each claim fails as a matter of law because, according to Apple, “not *once* in the 166-page pleading does a single Plaintiff identify any specific misrepresentation that he or she actually saw and relied upon in purchasing an Apple device.” ECF No. 395 at 23.

Plaintiffs’ misrepresentation claims are subject to Rule 9(b)’s requirement that fraud claims be pleaded with particularity.¹³ Plaintiffs’ allegations must therefore include “an account of the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations.” Swartz v. KPMG LLP, 476 F.3d 756, 765 (9th Cir. 2007). The purpose of this requirement is to provide the defendant with adequate notice of the claims against it; plaintiffs must allege “what is false or misleading about a statement, and why it is false.” Vess v. Ciba-Geigy Corp. USA, 317 F.3d 1097, 1106 (9th Cir. 2003) (quoting In re GlenFed, Inc. Sec. Litig., 42 F.3d 1541, 1548 (9th Cir. 1994)).

Plaintiffs must also adequately plead injury and causation. To have standing under the UCL, a plaintiff must have suffered an injury in fact and “lost money or property as a result of

practice possible, but it also allows for developers to ask for permission first, rendering the tool “neutral” in nature.

¹³ Rule 9(b) does not apply to Plaintiffs’ UCL claims for “unlawful” business practices to the extent these claims are grounded on something other than fraud.

such unfair competition.” Hall v. Time Inc., 158 Cal. App. 4th 847, 849 (2008). The standing requirement is substantially similar in this context for Plaintiff’s CLRA and FAL claims.¹⁴ See Kwikset Corp. v. Super. Ct., 51 Cal. 4th 310, 322 (2011) (a plaintiff must “establish a loss or deprivation of money or property sufficient to qualify as injury-in-fact” under the UCL and FAL); Meyer v. Sprint Spectrum L.P., 45 Cal. 4th 634, 646 (2009) (“[I]n order to bring a CLRA action, not only must a consumer be exposed to an unlawful practice, but some kind of damage must result.”). And for negligent misrepresentation claims, a plaintiff must establish detrimental reliance. For all of Plaintiffs’ misrepresentation claims, the parties agree that “[w]ithout such reliance, there is no recovery.” Bily v. Arthur Young & Co., 3 Cal. 4th 370, 413 (1992).

Nevertheless, “[w]hile a plaintiff must show that the misrepresentation was an immediate cause of the injury-producing conduct, the plaintiff need not demonstrate it was the only cause.” In re Tobacco II Cases, 46 Cal. 4th 298, 326 (2009). “Moreover, a presumption, or at least an inference, of reliance arises wherever there is a showing that a misrepresentation was material.” Engalla v. Permanente Med. Grp., Inc., 15 Cal. 4th 951, 977 (1997). A misrepresentation is material if a reasonable person “would attach importance to its existence or nonexistence in determining his choice of action in the transaction in question”; materiality is therefore ordinarily a question of fact unless the “fact misrepresented is so obviously unimportant that the jury could not reasonably find that a reasonable man would have been influenced by it.” Id. (quotations and citations omitted).

1. Specific Representations

In many consumer fraud cases, courts require a plaintiff to identify and describe the specific alleged misrepresentations that each plaintiff saw or heard, and upon which each plaintiff relied. Indeed, in granting Apple’s first motion to dismiss Plaintiff Pirozzi’s complaint, Judge Gonzalez Rogers held that Pirozzi’s failure to “provide the particulars of her own experience

¹⁴ Whether a party has Article III standing to bring a cause of action in federal court is a different analysis than whether the plaintiff has adequately established statutory standing under California’s UCL, CLRA, or FAL. Two Jinn, Inc. v. Gov’t Payment Serv., Inc., No. 09-CV-2701-JLS, 2010 WL 1329077, at *3 (S.D. Cal. Apr. 1, 2010).

reviewing or relying upon any” of the misrepresentations identified in her complaint was fatal to her claims. Pirozzi I, 913 F. Supp. 2d at 850. This Court denied Apple’s second motion to dismiss based on Pirozzi’s identification of the specific representations she saw and relied upon, which representations are also alleged here. Pirozzi II, 2013 WL 4029067, at *6–7. Apple now argues that the Court’s prior order was based on a misreading of Pirozzi’s allegations and renews its motion to dismiss.

Having again examined Pirozzi’s allegations, the Court now concludes that its prior decision regarding reliance was in error. In her Second Amended Complaint, Pirozzi alleged that Apple’s website contained the same representations discussed here, including the representation that “[a]ll apps run in a safe environment, so a website or app can’t access data from other apps.”¹⁵ Pirozzi II, 2013 WL 4029067, at *7. In its Order, the Court stated: “Plaintiff also alleges that she relied on that statement in making her purchasing decision.” Id. In actuality, however, Pirozzi did not allege that she relied on the statement; rather, she alleged only that she “visited Apple’s website,” not that she read the particular representations she alleged were misleading. Pirozzi v. Apple Inc., No. 12-cv-1529-JST, ECF No. 29 ¶ 10 (filed Jan. 22, 2013). Therefore, Pirozzi’s allegations of reliance were inadequate.

The CAC suffers from the same defect. It repeats the identical allegations made in Pirozzi’s Second Amended Complaint, and repeats the allegation that Pirozzi “viewed the Apple website.” CAC ¶¶ 121–25. In the next paragraph, the CAC further alleges: “Likewise, each of the other Plaintiffs visited Apple’s website” What the CAC fails to do is connect any specific Plaintiff to any specific representation. The Court now concludes, even reading the complaint in the light most favorable to Plaintiffs, that Plaintiffs have failed to allege that any one of them saw any particular representation.

¹⁵ The Court rejects Apple’s argument that this statement is not actionable because it is literally true. The CAC alleges that, although it comes pre-loaded on iDevices, the Contacts app is an app like any other.

2. Pleading a Long-Term and Extensive Advertising Campaign

Recognizing that the few specific representations relied upon by this Court in denying Apple's second motion to dismiss Pirozzi's complaint form a narrow basis upon which to base this action, Plaintiffs now largely rest their misrepresentation claims on a different basis: that Apple allegedly engaged in a long-standing, widespread advertising campaign that created a reputation for safety and reliability. In re Tobacco II, 46 Cal. 4th at 328 ("where, as here, a plaintiff alleges exposure to a long-term advertising campaign, the plaintiff is not required to plead with an unrealistic degree of specificity that the plaintiff relied on particular advertisements or statements").

The named plaintiffs in In re Tobacco II alleged that the tobacco industry defendants conducted "a decades-long campaign of deceptive advertising and misleading statements about the addictive nature of nicotine and the relationship between tobacco use and disease." Id. at 306. In concluding that the plaintiffs did not need to identify the specific statements upon which they relied, the California Supreme Court relied in part on a similar decision in Whiteley v. Philip Morris Inc., 117 Cal. App. 4th 635, 680–82 (2004).

In Whiteley, the California Court of Appeal affirmed a jury verdict in favor of the plaintiff, the husband of a woman who was a smoker and died of lung cancer. The tobacco industry defendants argued on appeal that the plaintiff had failed to present sufficient evidence of reliance to support the verdict. In particular, the defendants argued, as Apple does here, "that the evidence did not show that Whiteley heard any *specific* misrepresentation or false promise made by either defendant." They further argued: "'it is not enough that the plaintiff heard the alleged misrepresentation at some unidentified time from some unidentified source. Instead, the plaintiff must identify a *specific* misrepresentation that was *actually communicated* to the plaintiff (directly or indirectly).'" Id. at 680. The Whiteley court expressly rejected that argument and held that the plaintiff "did not have to prove that she saw or heard any specific misrepresentations of fact or false promises that defendants made or that she heard them directly from defendants or their agents. It was sufficient that the statements were issued to the public with the intent that they reach smokers and potential smokers and that Whiteley, as a member of the intended target

1 population, heard them.” Id. at 680–81.

2 Relying on section 533 of the Restatement Second of Torts, the court held that the trial
3 court had correctly instructed the jury on this question as follows: “One who makes a
4 misrepresentation or false promise or conceals a material fact is subject to liability if he or she
5 intends that the misrepresentation or false promise or concealment of a material fact will be passed
6 on to another person and influence such person's conduct in the transaction involved One
7 who makes a misrepresentation or false promise or conceals a material fact with the intent to
8 defraud the public or a particular class of persons is deemed to have intended to defraud every
9 individual in that category who is actually misled thereby.” Id. at 681. The Whiteley court
10 affirmed the jury’s verdict in favor of the plaintiff because the tobacco defendants’ statements

11 were intended to reassure smokers and potential smokers about the
12 health hazards of smoking and to convey that safety message. That
13 was exactly the message Whiteley received. Defendants' and their
14 agents' multifarious misrepresentations regarding the unsettled state
15 of knowledge and the unreliability of any link between cigarette
16 smoking and serious disease were made with the intention and
expectation that these misrepresentations would circulate among and
influence the conduct of all smokers and prospective smokers. They
were heard by or passed on to Whitel[e]y, who believed them.

17 Id. at 681–82.

18 While several courts have considered whether to apply Tobacco II so as to relieve an
19 individual plaintiff of the need to plead that she viewed and relied on a specific misrepresentation,
20 the cases in the aggregate do not define any bright line rules. A review of the jurisprudence,
21 however, has led the Court to identify the following factors in determining whether to apply
22 Tobacco II.

23 First, to state the obvious, a plaintiff must allege that she actually saw or heard the
24 defendant’s advertising campaign. See, e.g., Pfizer Inc. v. Super. Ct., 182 Cal. App. 4th 622, 632
25 (2010) (“[A]lthough Pfizer ran four different television commercials with the ‘as effective as
26 floss’ campaign, the commercials did not run continuously and there is no evidence that a majority
27 of Listerine consumers viewed any of those commercials.”); Herrington, 2010 WL 3448531, at *8
28 (“Plaintiffs have not plead that they viewed any of Defendants' advertising, let alone a ‘long-term

advertising campaign' by Defendants"); Delacruz v. Cytosport, Inc., No. 11-cv-3532-CW, 2012 WL 2563857, at *9 (N.D. Cal. June 28, 2012) ("Cytosport II") ("Plaintiff has not alleged reliance in connection with the advertising campaign because she has not claimed that she saw and relied on any of the advertising, apart from the product websites and television ads").

Second, the advertising campaign at issue should be sufficiently lengthy in duration, and widespread in dissemination, that it would be unrealistic to require the plaintiff to plead each misrepresentation she saw and relied upon. Compare Tobacco II, 46 Cal. 4th at 306 (plaintiffs excused from pleading specific reliance where advertising campaign lasted for "decades"); Comm. On Children's Television, Inc. v. Gen. Foods Corp., 35 Cal. 3d 197, 205–07 (1983) (superseded on other grounds) (advertising campaign was on television daily and lasted four years),¹⁶ with In re iPhone 4S, 2013 WL 3829653, at *12 ("The campaign was only about six months old when the CCAC was filed Plaintiffs have not alleged that the campaign here was comparable to that at issue in Tobacco II."); Delacruz v. Cytosport, Inc., No. 11-cv-3532-CW, 2012 WL 1215243, at *8 (N.D. Cal. Apr. 11, 2012) ("Cytosport I") ("Plaintiff has failed to allege that Defendant's advertising campaign approached the longevity and pervasiveness of the marketing at issue in Tobacco II"); Cytosport II, 2012 WL 2563857, at *9 ("The additional allegations regarding the scope of the advertising campaign do not establish that the advertising campaign was as lengthy or pervasive as the tobacco campaign"); In re Yasmin & Yaz (Drospirenone) Mktg., Sales Practices & Products Liab. Litig., No. 09-md-02100-DRH, 2012 WL 865041, at *9 n.20 (S.D. Ill. Mar. 13, 2012) (in class certification context, distinguishing Tobacco II because advertising campaign lasted only eighteen months and involved two advertisements and one corrective advertisement that may have been viewed by class members). How long and how extensive the advertising campaign must be is a fact-intensive inquiry; some campaigns will be too short, such as the six-

¹⁶ Children's Television was decided before Tobacco II, but is included here because it employs a similar analysis. The court there found that in light of defendants' "large scale program of deceptive advertising in which the specific advertisements change constantly," it would be impractical to require plaintiffs to plead the specifics of each advertisement. Children's Television, 35 Cal. 3d at 214.

1 month campaign in iPhone 4S, and others will be insufficiently extensive, such as the two
2 advertisements in In re Yasmin & Yaz, published over the course of eighteen months.

3 Third, a plaintiff seeking to take advantage of the exception should describe in the
4 complaint, and preferably attach to it, a “representative sample” of the advertisements at issue in
5 order adequately to notify the defendant of the precise nature of the misrepresentation claim —
6 that is, what, in particular, the defendant is alleged to have said, and how it was misleading. For
7 example, in Children's Television, 35 Cal. 3d at 205–07, the court held that a trial court “could
8 reasonably require plaintiffs to set out or attach a representative selection of advertisements, to
9 state the misrepresentations made by those advertisements, and to indicate the language or images
10 upon which any implied misrepresentations are based.” Id. at 218. In the California Supreme
11 Court’s view, that requirement “represents a reasonable accommodation between defendants’ right
12 to a pleading sufficiently specific ‘that the court can ascertain for itself if the representations . . .
13 were in fact material, and of an actionable nature,’ and the importance of avoiding pleading
14 requirements so burdensome as to preclude relief in cases involving multiple misrepresentations.”
15 Id. (citation omitted).

16 Fourth, the degree to which the alleged misrepresentations contained within the advertising
17 campaign are similar to each other, or even identical, is also an important factor.¹⁷ For example,
18 in Ticketmaster L.L.C. v. RMG Technologies, No. 07-cv-2534-ABC, 2007 WL 2989504, at *3
19 (C.D. Cal. Oct. 12, 2007), Ticketmaster alleged that the defendant had marketed and sold an
20 application that enabled customers to violate the Terms of Use and circumvent the security
21 measures on Ticketmaster’s website by purchasing large quantities of tickets. Because the
22 complaint adequately alleged that the defendant aided and abetted its customers’ “same false
23 promise” thousands of times, the court held it was not necessary for the plaintiff to identify “each
24 instance of this alleged fraud, or each and every individual involved.” Instead, it was sufficient to
25 identify “to the extent possible the persons involved . . . and set out a time frame for the repeated
26 misrepresentations.” Id. Although Ticketmaster did not arise in the advertising context, it

27
28 ¹⁷ This does not mean that the representations must be identical. In both Children’s Television and
Tobacco II, the advertisements at issue were “similar by category.”

nevertheless provides helpful guidance for the Court in determining the circumstances that may allow a plaintiff to exercise the advertising campaign exception recognized in In re Tobacco II. Indeed, the decision in In re Tobacco II, itself, yields the rule that if a plaintiff alleges a long-term advertising campaign, the advertisements at issue should be similar enough to be considered as part of one campaign, or the delivery of a single message or set of messages, rather than a disparate set of advertising content published in the ordinary course of commerce.

Fifth, in the absence of specific misrepresentations, a complaint subject to Rule 9(b)'s requirements should plead with particularity, *and separately*, when and how each named plaintiff was exposed to the advertising campaign. It is not sufficient to plead as a group, nor is it sufficient simply to allege general exposure without more detail. The facts in In re Tobacco II contained such detail. So too in Morgan v. AT&T Wireless Servs., Inc., 177 Cal. App. 4th 1235, 1257–58 (2009), where the plaintiffs alleged that when considering purchasing T68i mobile phones from AT&T Wireless, “they each conducted research in which they encountered AT&T advertisements and press releases explaining the advanced features of the T68i and the improvements AT&T was making and was going to make to its GSM/GPRS network.” They also alleged they were exposed to similar representations at the AT&T store when they purchased their phones and service plans, “and that they relied upon their research (including information from the AT&T advertisements and press releases, and the in-store representations) in deciding to purchase the T68i from AT&T.” Id. Within a “relatively short period of time” after purchasing their phones, and despite AT&T’s marketing concerning the upgrades to its network, AT&T performed upgrades on the network that it knew would render the T68i phones “essentially useless.”

AT&T moved to dismiss because the plaintiffs had failed to identify specific misrepresentations. The court held that the allegations supported the plaintiffs’ various misrepresentation claims, including the UCL, CLRA, FAL, and common law fraud, because the plaintiffs

were not required, as AT&T asserts, to plead the specific advertisements or representations they relied upon in making their decisions to purchase the T68i Although the advertising campaign alleged in this case was not as long-term a campaign as the tobacco companies’ campaign discussed in Tobacco II, it is

1 alleged to have taken place over many months, in several different
2 media, in which AT&T consistently promoted its GSM/GPRS
3 network as reliable, improving, and expanding.

4 Id. In the context of the common law fraud claim, the court again observed: “where a fraud claim
5 is based upon numerous misrepresentations, such as an advertising campaign that is alleged to be
6 misleading, plaintiffs need not allege the specific advertisements the individual plaintiffs relied
7 upon; it is sufficient for the plaintiff to provide a representative selection of the advertisements or
8 other statements to indicate the language upon which the implied misrepresentations are based.”

9 Id. at 1262.

10 The detail the Court requires here ensures that the advertisements at issue are
11 representations that consumers were likely to have viewed, as opposed to representations that were
12 isolated or more narrowly disseminated, such as statements buried on a rarely-viewed webpage, or
13 made on an investor phone conference. Certainly, such representations could be part of an
14 advertising campaign, but the complaint should describe the mechanism of dissemination for all
15 identified representations.

16 Sixth, the court must be able to determine when a plaintiff made her purchase or otherwise
17 relied in relation to a defendant’s advertising campaign, so as to determine which portion of that
18 campaign is relevant. Representations made prior to purchase are relevant to a plaintiff’s claim;
19 ones made after are not. Consequently, a plaintiff should describe, to the best of her ability, (1)
20 when the product was purchased, (2) the timeframe of the advertisements at issue, and (3) when
21 the plaintiff was exposed to the advertisements.

22 These factors are merely one court’s attempt to harmonize the developing jurisprudence of
23 false advertising claims. Future decisions from the California state and federal courts may reveal
24 additional factors, or demonstrate that some of those just listed are not helpful. Nevertheless,
25 these are the factors the Court has been able to identify.

26 Applying them here, the Court finds that Plaintiffs have not adequately alleged a long-term
27 advertising campaign of the kind that would excuse them from pleading specific reliance.

28 Although Plaintiffs allege a long-term advertising campaign, they fail to do so with the level of

1 detail that has led other courts to allow such claims to proceed.

2 First, as set forth above, it is not clear that any of the plaintiffs were actually exposed to
3 Apple's advertising campaign.

4 Second, although the CAC alleges with sufficient specificity the *length* of the advertising
5 campaign at issue — it alleges that the campaign began at least by 2008 and continued up through
6 the filing of the CAC — it does not contain sufficient detail concerning the *extent* of the
7 advertising. It is unclear from the CAC how often the advertisements were published, or in which
8 media. Without more detail, the Court cannot conclude that it would be “unrealistic” to require
9 Plaintiffs to plead with specificity their exposure to each alleged misrepresentation.

10 Third, and relatedly, Plaintiffs have not attached or described a “representative sample” of
11 the advertisements at issue. Instead of cursory allegations that Apple “repeatedly represented that
12 Apple's products are safe and secure, and that private information could not be accessed by third-
13 party apps without the user's express consent,” CAC ¶ 64, Plaintiffs should describe in detail, or
14 attach, advertisements that they contend are typical of the advertising campaign at issue. The
15 Court is mindful that Plaintiffs have identified some specific representations contained on Apple's
16 website, or made by Apple's employees, including its former and current CEOs. But it is not
17 enough. After reading the complaint asserted against it, a defendant should be able to understand
18 which advertising is alleged to be misleading, and how it is misleading, so that it may prepare a
19 defense and identify in discovery the remainder of the advertising at issue — and just as
20 importantly, that advertising which is not at issue. It is only through this process that the parties
21 will be able to cabin, and then narrow, the scope of the litigation in succeeding stages. Because
22 Plaintiffs have failed to allege in sufficient detail the nature of the advertisements, the Court finds
23 that the CAC does not adequately notify Apple of the precise nature of the misrepresentation
24 claims asserted against it.

25 Fourth, because there is insufficient detail with respect to the advertising at issue, the Court
26 cannot conclude that the alleged misrepresentations are sufficiently similar to each other to
27 constitute a single campaign, message, or set of messages susceptible to uniform treatment.

28 Fifth, Plaintiffs do not separately allege in any detail how they were exposed to Apple's

1 advertising campaign. It is not enough merely to allege that Plaintiffs “viewed Apple’s website,
2 saw in-store advertisements, and/or [were] aware of Apple’s representations regarding the safety
3 and security of the iDevices prior to purchasing their own iDevices.” CAC ¶ 126.

4 Finally, without engaging Apple’s attempts to develop a factual record at the pleading
5 stage, the Court is mindful of the fact that Plaintiffs have not alleged when they purchased their
6 devices, other than to allege they were all purchased prior to February 2012. Consequently, even
7 if Plaintiffs adequately address the other deficiencies in the CAC, it would still be difficult for the
8 Court to conclude that Plaintiffs were exposed to the advertising at issue prior to purchasing their
9 iDevices without more detailed allegations concerning the chronology of events for each Plaintiff
10 in this case.

11 **3. Failure to Disclose**

12 Plaintiffs argue in the alternative that their misrepresentation claims are viable because
13 Apple had an affirmative duty to disclose material facts of which it had exclusive knowledge, *i.e.*,
14 the vulnerability of Plaintiffs’ iDevices to the theft of their address books by third party apps,
15 rendering it unnecessary for Plaintiffs to identify any misrepresentations.

16 “As the Ninth Circuit has recently cautioned, in the context of product defect claims,
17 ‘California courts have generally rejected a broad duty to disclose.’” Donohue v. Apple, Inc., 871
18 F. Supp. 2d 913, 925 (N.D. Cal. 2012) (citing Wilson v. Hewlett-Packard Co., 3d 1136, 1141 (9th
19 Cir. 2012). Nondisclosure or concealment constitutes actionable fraud in only four circumstances:
20 “(1) when the defendant is in a fiduciary relationship with the plaintiff; (2) when the defendant had
21 exclusive knowledge of material facts not known to the plaintiff; (3) when the defendant actively
22 conceals a material fact from the plaintiff; and (4) when the defendant makes partial
23 representations but also suppresses some material facts.” LiMandri v. Judkins, 52 Cal. App. 4th
24 326, 336 (1997).

25 Plaintiffs argue that their non-disclosure claims fit into each of the last three categories.
26 Because the Court has already determined above that Plaintiffs do not adequately identify Apple’s
27 alleged misrepresentations, only the second and third categories are at issue.

28 But Plaintiffs’ failure to disclose claims have a separate problem: “[a] manufacturer’s

duty to consumers is limited to its warranty obligations absent either an affirmative misrepresentation or a safety issue.” Donohue, 871 F. Supp. 2d at 925(quoting Oestreicher v. Alienware Corp., 322 F. App'x 489, 493 (9th Cir. 2009)).¹⁸ Here, Plaintiffs fail to allege when they purchased their iDevices, when the alleged defects arose, what kind of warranty Apple provided, the terms of the warranty, and the warranty's duration. Consequently, the Court is unable to conclude whether the alleged defect manifested within the warranty period, and therefore cannot sustain Plaintiffs' claims.

Because Plaintiffs have failed to plead with particularity the specific representations upon which they relied, have failed adequately to plead a long-term and extensive advertising campaign, and have failed to satisfy the requirements for a pure nondisclosure or concealment claim, the Court will grant Apple's motion to dismiss Plaintiffs' UCL, FAL, CLRA, and negligent misrepresentation claims, with leave to amend.

D. California Comprehensive Computer Data Access and Fraud Act

The California Comprehensive Computer Data Access and Fraud Act (“CDAFA”), Cal. Penal Code § 502, “expand[s] the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.” Id. § 502(a). Every Plaintiff except Pirozzi asserts a claim against Apple for violation of the CDAFA. The CDAFA imposes liability, *inter alia*, on any person who

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network

¹⁸ Once the warranty expires, a manufacturer does not have an affirmative duty to disclose a latent defect unless it poses an “unreasonable safety hazard.” See Donohue, 871 F. Supp. 2d at 926; Wilson, 668 F.3d at 1141–43.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

Id. § 502(c)(1),(2),(6)–(8). The CDAFA authorizes the owner of the computer “who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) [to] bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief.” Id. § 502(e)(1).

Apple moves to dismiss on several grounds. As an initial matter, the Court notes that, to the extent Plaintiffs’ theories of liability under the CDAFA derive from Apple’s “reviewing, editing, and deciding whether to” make available to its users the offending apps, those claims are barred by the Communications Decency Act, as discussed above.

To the extent Plaintiffs assert a CDAFA claim based on Apple’s encouragement of the development of the offending features of the subject apps, those allegations are insufficiently pleaded. Each subsection of the statute Plaintiffs assert incorporates expressly or by reference a requirement that the defendant acted “without permission.” See Cal. Pen. Code § 502(b)(10) (defining “computer contaminant”). Courts in this district have interpreted “without permission” to mean “in a manner that circumvents technical or code based barriers in place to restrict or bar a user’s access.” Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1036 (N.D. Cal. 2012). See also In re Google Android Consumer Privacy Litig., No. 11-mc-02264-JSW, 2013 WL 1283236, at *12 (N.D. Cal. Mar. 26, 2013); In re iPhone Application Litig. (“iPhone I”), No. 11-md-02250-LHK, 2011 WL 4403963, at *12–13 (N.D. Cal. Sept. 20, 2011).

Plaintiffs argue that their CDAFA claim is viable because they “did not know that the apps contained the malicious code at issue here.” ECF No. 421 at 42. Other courts in this district have already persuasively rejected this argument. See iPhone I, 2011 WL 4403963, at *12 (“On Plaintiffs’ own allegations, the iOS and third party apps — which contain the alleged ‘surreptitious

code’ — were all installed or updated *voluntarily* by Plaintiffs.”); In re Google Android Consumer Privacy Litig., 2013 WL 1283236, at *12 (“Plaintiffs, however, have not included any facts that show — or lead to a reasonable inference — that the tracking codes have been designed in such a way to render ineffective any barriers the Plaintiffs might wish to use to prevent access to their PII.”).

Plaintiffs’ allegations are materially indistinguishable from the allegations in iPhone I and In re Google Android Consumer Privacy. Although Plaintiffs allege they did not grant permission to the apps to copy their address books, there is no suggestion that the apps overcame “technical or code based barriers in place to restrict or bar a user’s access.” According to the CAC, the apps in question had open access to Plaintiffs’ address books.¹⁹

Plaintiffs’ CDAFA claims against Apple will be dismissed.

E. Strict Products Liability: Design Defect and Failure to Warn

The Opperman Plaintiffs assert design defect and failure to warn strict products liability claims against Apple. “A manufacturer is strictly liable in tort when an article he places on the market, knowing that it is to be used without inspection for defects, proves to have a defect that causes injury to a human being.” Anderson v. Owens-Corning Fiberglas Corp., 53 Cal. 3d 987, 994 (1991) (quoting Greenman v. Yuba Power Products, Inc., 59 Cal. 2d 57, 62 (1963)).

Importantly, “recovery under the doctrine of strict liability is limited solely to ‘physical harm to person or property.’” Jimenez v. Superior Court, 29 Cal. 4th 473, 482 (2002) (quoting Seely v. White Motor Co., 63 Cal. 2d 9, 18 (1965)). “Damages available under strict products liability do not include economic loss, which includes damages for inadequate value, costs of repair and replacement of the defective product or consequent loss of profits — without any claim

¹⁹ The Court recognizes there is a split of authority in this district concerning the appropriate scope of the “without permission” language in the CDAFA. Weingand v. Harland Fin. Solutions, Inc., No. 11-cv-3109-EMC, 2012 WL 2327660, at *5 (N.D. Cal. June 19, 2012). Even Weingand, however, still requires that Defendants have circumvented “restrictions on access” of some kind. The CAC does not allege that the subject apps circumvented any restrictions at all. Instead, it alleges that Apple failed to implement any such restriction, thereby enabling the App Defendants to copy Plaintiffs’ address books. Under either approach to the CDAFA, Plaintiffs fail to state a viable claim.

of personal injury or damages to other property” Id. (quotation marks and citations omitted). By contrast, “[t]he law of contractual warranty governs damage to the product itself.” Id. at 483.

Plaintiffs do not explain what injury they allege that satisfies the economic loss rule. The CAC alleges only that “Plaintiffs suffered personal injuries as a result of the defective design, including invasions of their privacy and damages to their properties (the mobile address books).” CAC ¶ 694. Those injuries are not “physical harm to person or property” and cannot support a products liability claim. For this reason, the Court will dismiss Plaintiffs’ strict products liability claim.

F. Negligence

Plaintiffs’ negligence claims are barred by the economic loss rule discussed in the immediately previous section. “Purely economic damages to a plaintiff which stem from disappointed expectations from a commercial transaction must be addressed through contract law; negligence is not a viable cause of action for such claims.” iPhone II, 844 F. Supp. 2d at 1064.

The Court will dismiss Plaintiffs’ negligence claim against all Defendants.

G. RICO

Plaintiffs state that they “elect not to prosecute [the RICO] claim at this time and have no objection to its dismissal without prejudice as to” Apple. ECF No. 421 at 50. The Court construes Plaintiffs’ statement as a Rule 41(a)(1)(A)(i) notice of voluntary dismissal, which is self-executing.

H. Aiding and Abetting

In response to Apple’s argument that aiding and abetting is not a stand-alone cause of action in California, Plaintiffs respond: “The fact that Plaintiffs’ aiding and abetting allegations are set out in a separate claim merely provides clarity to the complaint by specifying that Plaintiffs contend that Apple is liable not just for its own actions but for those of the App Defendants.” ECF No. 421 at 49. Far from providing clarity, the separate aiding and abetting count casts in doubt which claims that, facially, are asserted only against the App Defendants are also meant to apply to Apple as well. The Court cannot discern from the CAC what additional liability, other than the claims Plaintiffs explicitly assert against Apple, Plaintiffs attempt to impose on Apple by virtue of

the aiding and abetting count. For this reason, the Court will dismiss the claim. Plaintiffs are advised that each claim in the complaint should clearly set forth against which Defendants it is meant to be asserted.

IV. APP DEFENDANTS' MOTIONS TO DISMISS

Like Apple, the App Defendants move to dismiss all of Plaintiffs' claims against them on Article III standing grounds, as well as pursuant to Rule 12(b)(6).²⁰

A. Article III Standing

The Article III standing analysis as applied to Plaintiffs' claims against the App Defendants differs from the analysis regarding Plaintiffs' claims against Apple. In particular, the App Defendants argue that Plaintiffs have failed to identify an injury-in-fact sufficient to establish standing.

In evaluating Path's motion to dismiss the Hernandez complaint prior to the relation of that action to the above-captioned action, Judge Gonzalez Rogers evaluated the alleged injury of "diminished mobile device resources, such as storage, battery life, and bandwidth."²¹ Hernandez v. Path, Inc., No. 12-cv-01515-YGR, 2012 WL 5194120, at *1–2 (N.D. Cal. Oct. 19, 2012). She found that the diminished mobile device resources injury was *de minimis*. Id. The allegations in the CAC provide no further detail concerning this alleged injury, but instead recast it similar terms. See, e.g., CAC ¶ 147 ("For instance, the unauthorized transmissions and operations used iDevice resources, battery life, energy and cellular time at a cost to Plaintiffs and caused loss of use and enjoyment of some portion of each iDevice's useful life."). There is no indication, for example, that battery resources were depleted as in iPhone II. Because Plaintiffs have not quantified or otherwise articulated the alleged resource usage, they fail to allege an injury that can serve as the basis of standing. See, e.g., In re Google, Inc. Privacy Policy Litig., No. 12-cv-01382-

²⁰ The App Defendants also repeat some of the arguments Apple makes, for example that those Plaintiffs who are not from California cannot sue under California law. See ECF No. 393 at 7. Where the Court has already addressed an identical argument in the section on Apple's motion to dismiss, it does not do so again here.

²¹ Judge Gonzalez Rogers also evaluated two other types of alleged injury that Plaintiffs no longer allege and that are not germane to this Order.

1 PSG, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013) (distinguishing Hernandez because resource
2 usage was significant and “systemic rather than episodic”).

3 In addition, however, Plaintiffs present four new theories of injury-in-fact not present in
4 Hernandez. First, Plaintiffs argue that their claim for injunctive relief is sufficient to confer
5 standing. “To have standing to assert a claim for prospective injunctive relief, a plaintiff must
6 demonstrate ‘that he is realistically threatened by a repetition of [the violation].’” Melendres v.
7 Arpaio, 695 F.3d 990, 997 (9th Cir. 2012) (quoting City of Los Angeles v. Lyons, 461 U.S. 95,
8 109 (1983)). Here, Plaintiffs allege that the App Defendants all discontinued their practices when
9 the practice of transmitting user address books was made public. Moreover, Plaintiffs allege that
10 Apple has instituted additional privacy controls that enable users to control which apps have
11 access to their address books. Because there is no realistic threat of repetition, Plaintiffs cannot
12 establish standing through their prayer for injunctive relief.

13 Second, Plaintiffs argue that the App Defendants interfered with their property rights in
14 their address books, conferring standing on Plaintiffs to sue. “[D]istrict courts have been reluctant
15 to find standing based *solely* on a theory that the value of a plaintiff’s [personal information] has
16 been diminished.” Yunker v. Pandora Media, Inc., No. 11-cv-03113-JSW, 2013 WL 1282980
17 (N.D. Cal. Mar. 26, 2013). “[I]njury-in-fact in this context requires more than an allegation that a
18 defendant profited from a plaintiff’s personal identification information. Rather, a plaintiff must
19 allege how the defendant’s use of the information deprived the plaintiff of the information’s
20 economic value. Put another way, a plaintiff must do more than point to the dollars in a
21 defendant’s pocket; he must sufficiently allege that in the process he lost dollars of his own.” In re
22 Google, Inc. Privacy Policy Litig., 2013 WL 6248499, at *5. See also In re Google Android
23 Consumer Privacy Litig., 2013 WL 1283236, at *4 (“Similarly, although Plaintiffs allege that a
24 market exists that could provide them the opportunity to sell their PII, *none* of the Plaintiffs
25 specifically tie those allegations to them. Plaintiffs also do not allege they attempted to sell their
26 personal information, that they would do so in the future, or that they were foreclosed from
27 entering into a value for value transaction relating to their PII, as a result of the Google
28

Defendants' conduct.”).²²

Plaintiffs here have failed to allege any details concerning their argument that their address books’ value was diminished by the App Defendants’ conduct. Instead, Plaintiffs argue that address books are distinct from the “automatically-generated computer data sets” at issue in the multitude of cases in which courts have found allegations similar to Plaintiffs insufficient. The distinction is one without a difference. Whether automatically-generated or generated by the user, Plaintiffs must “tie” their allegations that their personal information has value to the alleged injury they suffered. Here, Plaintiffs have failed to do so. Consequently, Plaintiffs do not have Article III standing based on injury to their property rights.

However, Plaintiffs’ two remaining theories of injury are sufficient to confer standing. First, as observed above, Plaintiffs are able to establish standing through their statutory claims, because “[t]he injury required by Article III can exist solely by virtue of ‘statutes creating legal rights, the invasion of which creates standing.’” Edwards v. First Am. Corp., 610 F.3d 514, 517 (9th Cir. 2010) (quoting Fulfillment Servs. Inc. v. United Parcel Serv., Inc., 528 F.3d 614, 618 (9th Cir. 2008)). See In re Google, Inc. Privacy Policy Litig., 2013 WL 6248499, at *8 (“Although Article III always requires an injury, the alleged violation of a statutory right that does not otherwise require a showing of damages is an injury sufficient to establish Article III standing.”).

Second, Plaintiffs assert a common law claim for invasion of privacy. Regardless of the merits of that claim, the Court finds Plaintiffs’ allegations sufficient on this point. The essence of the standing inquiry is to determine whether the plaintiff has “alleged such a personal stake in the outcome of the controversy as to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends.” Baker v. Carr, 369 U.S. 186, 204 (1962). It is

²² The Court does not read these decisions to be holding that consumers do not have property rights in their electronically stored private information, but that the copying of such information without any meaningful economic injury to consumers is insufficient to establish standing on that basis. Cf. FMC Corp. v. Capital Cities/ABC, Inc., 915 F.2d 300, 303–04 (7th Cir. 1990) (applying California law; noting that “[i]n cases where the alleged converter has only a copy of the owner's property and the owner still possesses the property itself, the owner is in no way being deprived of the use of his property. The only rub is that someone else is using it as well.”).

beyond meaningful dispute that a plaintiff alleging invasion of privacy as Plaintiffs do here presents a dispute the Court is permitted to adjudicate. See, e.g., Wright & Miller, 13A Fed. Prac. & Proc. Juris. § 3531.4 (3d ed.); Ruiz v. Gap, Inc., 380 F. App'x 689, 691 (9th Cir. 2010) (unpublished) (holding allegation that laptop theft put plaintiff at “greater risk of identity theft” was sufficient injury, even where plaintiff had no UCL standing); Yunker, 2013 WL 1282980, at *6 (finding Article III standing based on violation of constitutional privacy rights); Citizens for Health v. Leavitt, 428 F.3d 167, 176 & n.9 (3d Cir. 2005), cert. den'd 127 S. Ct. 43 (2006) (holding Plaintiffs had standing to challenge “Privacy Rule” that allowed medical providers to use or disclose personal health information without patient consent because summary judgment evidence showed “at least one individual plaintiff’s health information has been, or will imminently be, disclosed without her consent by private health care providers and drugstore chains”); Folgelstrom v. Lamps Plus, Inc., 195 Cal. App. 4th 986, 990 (2011) (discussing invasion of privacy claims). The App Defendants do not respond to this theory of injury. The Court finds it is sufficient to confer standing for those claims on which the injury bears — intrusion upon seclusion and public disclosure of private facts.

For the foregoing reasons, the Court will dismiss Plaintiffs’ common law claims against the App Defendants, except their invasion of privacy claims, on standing grounds.

B. Plaintiffs' UCL Claims

The Court will also dismiss Plaintiffs’ UCL claims against the App Defendants, because, in order to have standing to assert their UCL claims, Plaintiffs must show that they “lost money or property,” and, as the Court concludes above, they have failed to make such a showing. See Kwikset Corp. v. Super. Ct., 51 Cal. 4th 310, 325 (2011).

C. Invasion of Privacy: Intrusion Upon Seclusion

The Opperman Plaintiffs assert the common law claim of intrusion upon seclusion against the App Defendants. In particular, Plaintiffs allege that “[b]y surreptitiously obtaining, improperly gaining knowledge, reviewing and retaining Plaintiffs’ private mobile address books (or substantial portions thereof), the App Defendants intentionally intruded on and into each respective Plaintiff’s solitude, seclusion or private affairs.” CAC ¶ 630. Plaintiffs allege the

1 intrusion was “highly offensive to a reasonable person,” as evidenced by the “myriad newspaper
2 articles, blogs, op eds., and investigative exposes’ [that] were written complaining and objecting
3 vehemently to these defendants’ practices.” CAC ¶ 631. Plaintiffs also allege that
4 “[c]ongressional inquiries were opened to investigate these practices and some defendants even
5 publicly apologized. The surreptitious manner in which the App Defendants’ conducted these
6 intrusions confirms their outrageous nature.” Id.

7 The Second Restatement of Torts provides: “One who intentionally intrudes, physically or
8 otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to
9 liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a
10 reasonable person.” Rest. (2d) of Torts § 652B (1977). California courts recognize that ““a
11 measure of personal isolation and personal control over the conditions of its abandonment is of the
12 very essence of personal freedom and dignity, is part of what our culture means by these
13 concepts.”” Shulman v. Grp. W Prods., Inc., 18 Cal. 4th 200, 231 (1998) (quoting Bloustein,
14 Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, 39 N.Y.U. L.Rev. 962, 973–
15 974 (1964) (footnote omitted)).

16 An intrusion upon seclusion claim “does not depend upon any publicity given to the person
17 whose interest is invaded or to his affairs.” Rest. (2d) of Torts § 652B, Comment a. Nor must the
18 intrusion be physical:

19 it may be performed by the use of the defendant's senses, with or
20 without mechanical aids, to oversee or overhear the plaintiff's
21 private affairs, as by looking into his upstairs windows with
22 binoculars or tapping his telephone wires. It may be by some other
23 form of investigation or examination into his private concerns, as by
24 opening his private and personal mail, searching his safe or his
25 wallet, examining his private bank account, or compelling him by a
26 forged court order to permit an inspection of his personal
27 documents. The intrusion itself makes the defendant subject to
28 liability, even though there is no publication or other use of any kind
of the photograph or information outlined.

26 Id., Comment b. California has adopted the Restatement’s two-prong formulation of intrusion
27 upon seclusion claims: “(1) intrusion into a private place, conversation or matter, (2) in a manner
28 highly offensive to a reasonable person.” Shulman, 18 Cal. 4th at 231.

1 “The tort is proven only if the plaintiff had an objectively reasonable expectation of
2 seclusion or solitude in the place, conversation or data source.” Id. Whether a legally protected
3 privacy interest is at stake is a question of law; whether a plaintiff has a reasonable expectation of
4 privacy and whether the defendant’s conduct is a serious invasion of privacy are mixed questions
5 of law and fact. See Hill v. Nat’l Collegiate Athletic Assn., 7 Cal. 4th 1, 39–40 (1994) (discussing
6 California constitutional invasion of privacy). “If the undisputed material facts show no
7 reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of
8 invasion may be adjudicated as a matter of law.” Id.

9 The Court does not read the App Defendants to be contesting that Plaintiffs have a legally
10 protectable privacy interest in their address books, nor do the App Defendants contest that the apps
11 intruded upon that interest. Instead, the App Defendants argue that Plaintiffs did not have a
12 reasonable expectation of privacy in the information, and that the intrusion was not sufficiently
13 offensive to give rise to a claim for intrusion upon seclusion.

14 **1. Reasonable Expectation of Privacy**

15 A claim for intrusion upon seclusion is not viable unless the plaintiff had an “objectively
16 reasonable expectation of seclusion or solitude in the place, conversation or data source.”
17 Shulman, 18 Cal. 4th at 231. Several factors affect a person’s reasonable expectation of privacy.
18 Advance notice of an impending action, customs, practices, and physical settings may “create or
19 inhibit reasonable expectations of privacy.” Hill, 7 Cal. 4th at 36. “Finally, the presence or
20 absence of opportunities to consent voluntarily to activities impacting privacy interests obviously
21 affects the expectations of the participant.” Id.

22 Here, there are two types of alleged intrusions at issue. Plaintiffs allege that some apps
23 copied Plaintiffs’ address books without consent or any prompt. The Court finds that Plaintiffs’
24 expectation of privacy in their address books contained on their iDevices in this circumstance was
25 reasonable. See, e.g., United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) (“[C]ell phones
26 contain a wealth of private information, including emails, text messages, call histories, address
27 books, and subscriber numbers. Zavala had a reasonable expectation of privacy regarding this
28 information.”); United States v. Cerna, No. 08-cv-0730-WHA, 2010 WL 5387694, at *6 (N.D.

Cal. Dec. 22, 2010) (citing Zavala) (“Luis Herrera had a reasonable expectation of privacy in the contents of the seized phones as his physical possession of the cell phones created a reasonable expectation of privacy in their contents.”); United States v. Chan, 830 F. Supp. 531, 534 (N.D. Cal. 1993) (criminal defendant had expectation of privacy in contents of pager because “[t]he expectation of privacy in an electronic repository for personal data is therefore analogous to that in a personal address book or other repository for such information”).

Other apps, such as Gowalla and Instagram, copied address books only after they prompted the user to “find friends” who use the same app by scanning Plaintiffs’ address books. See, e.g., CAC ¶¶ 238, 317. The menu prompts notified users that the app would scan their address books. Although the prompts required Plaintiffs to consent, Plaintiffs’ expectation of privacy in that circumstance was still reasonable. Plaintiffs allege that they would not have consented had they known that their apps would not only scan their address books to determine whether their friends were using the same app, but then upload the address books to the app developer for other purposes. Plaintiffs allege that their consent was obtained by fraud, and that their consent was therefore invalid. See Rest. (2d) of Torts § 892B (1979) (“If the person consenting to the conduct of another is induced to consent by a substantial mistake concerning the nature of the invasion of his interests or the extent of the harm to be expected from it and the mistake is known to the other or is induced by the other’s misrepresentation, the consent is not effective for the unexpected invasion or harm.”); Sanchez-Scott v. Alza Pharm., 86 Cal. App. 4th 365, 377–78 (2001) (sustaining intrusion upon seclusion claim where doctor obtained consent of patient to breast examination in front of a drug salesperson without disclosing salesperson was not a medical professional).

Here, Plaintiffs allege that the App Defendants obtained their consent by misrepresenting their purpose. That is, they allege that the App Defendants intentionally represented that they would only “scan” Plaintiffs’ address books for purposes of the “find friends” feature without disclosing that, at the same time, the app would transmit a copy of the address book to Defendants for their own use. Taking the allegations in the CAC as true, the Court concludes that Plaintiffs’ consent was invalid. Consequently, Plaintiffs had a reasonable expectation of privacy with respect

to the address books copied by each app at issue.

2. Offensiveness

The App Defendants' primary argument in support of their motion to dismiss Plaintiffs' intrusion upon seclusion claim is that the intrusion at issue is not "highly offensive."

Liability for intrusion upon seclusion will not lie "unless the interference with the plaintiff's seclusion is a substantial one, of a kind that would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object." Rest. (2d) of Torts § 652B, Comment d. "A court determining the existence of 'offensiveness' would consider the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded." Miller v. Nat'l Broad. Co., 187 Cal. App. 3d 1463, 1483–84 (1986).

In evaluating a claim for invasion of California's constitutional right to privacy, the iPhone II court held that the surreptitious tracking of personal data and geolocation information was not an "egregious breach of social norms." 844 F. Supp. 2d at 1063. In coming to that conclusion, that court relied primarily on the decision in Folgelstrom v. Lamps Plus, Inc., 195 Cal. App. 4th 986, 992 (2011). In Folgelstrom, the plaintiff alleged that the defendant retailer routinely asked for customers' zip codes, asked a credit agency to match their zip codes and credit card numbers to home mailing addresses, and then engaged in mail marketing using the addresses. The court first concluded that the plaintiffs did not have a legally protected private interest in their mailing addresses. The court also held that the retailer's conduct was not egregious, but "routine commercial behavior." Id. at 992.

The decision in Folgelstrom is distinguishable.²³ Here, Plaintiffs allege the theft of the

²³ The App Defendants also argue that Folgelstrom limited intrusion upon seclusion claims to conduct that involves a highly offensive *use* of the private information. See Folgelstrom, 195 Cal. App. 4th at 993 ("[W]e have found no case which imposes liability based on the defendant obtaining unwanted access to the plaintiff's private information which did not also allege that the *use* of plaintiff's information was highly offensive.").

That passage from Folgelstrom is dicta, and the Court has been unable to locate any other decision

information in their personal contact lists, which is more private than a person's mailing address. And while the Court recognizes that attitudes toward privacy are evolving in the age of the Internet, smartphones, and social networks, the Court does not believe that the surreptitious theft of personal contact information — which is what the CAC alleges — has come to be qualified as “routine commercial behavior.” Indeed, Plaintiffs allege that consumers, the media, the Federal Trade Commission, and Congress have closely scrutinized the practices at issue in this case because of concerns that the practices were inappropriate.

The Court cannot conclude as a matter of law that Defendants' copying of Plaintiffs' address books was not “highly offensive.” That question is best left for a jury.

3. Damages

The App Defendants briefly argue that Plaintiffs have failed adequately to allege damages from the alleged intrusion upon seclusion because they have failed to allege economic injury. No such allegation is required. A plaintiff who prevails on an intrusion upon seclusion claim may recover damages for “anxiety, embarrassment, humiliation, shame, depression, feelings of powerlessness, anguish, etc.” Operating Engineers Local 3 v. Johnson, 110 Cal. App. 4th 180, 187 (2003) (quoting Miller v. National Broadcasting Co., 187 Cal. App. 3d 1463, 1485 (1986)).

For the foregoing reasons, the Court will deny the App Defendants' motion to dismiss the Opperman Plaintiffs' claim for intrusion upon seclusion.

that has applied the limitation; it was not relied upon, for example, in iPhone II. Moreover, unlike the Folgelstrom court, this Court *has* been able to locate cases which impose liability without an allegation of highly offensive use. For example, in Sanchez-Scott v. Alza Pharm., 86 Cal. App. 4th 365, 377–78 (2001), a patient adequately stated an intrusion upon seclusion claim where her doctor performed a breast examination in front of a pharmaceutical salesperson without revealing that the salesperson was not a medical professional. In that case, no “highly offensive use” was at issue, only the highly offensive manner in which the privacy interest was invaded.

The Restatement also expressly disavows any such limitation. See Rest. (2d) of Torts § 652B, Comment b (“The intrusion itself makes the defendant subject to liability, even though there is no publication *or other use of any kind* of the photograph or information outlined.”) (emphasis added).

D. Invasion of Privacy: Public Disclosure of Private Facts

The Opperman Plaintiffs also assert an invasion of privacy claim for public disclosure of private facts.

The elements of a claim for public disclosure of private facts are: “(1) public disclosure, (2) of a private fact, (3) which would be offensive and objectionable to the reasonable person, and (4) which is not of legitimate public concern.” Taus v. Loftus, 40 Cal. 4th 683, 717 (2007) (quotation omitted). Here, Plaintiffs have failed to allege a public disclosure.

The Restatement makes clear that Plaintiffs must allege disclosure to the public “at large”:

“Publicity,” as it is used in this Section, differs from “publication,” as that term is used in § 577 in connection with liability for defamation. “Publication,” in that sense, is a word of art, which includes any communication by the defendant to a third person. “Publicity,” on the other hand, means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge. The difference is not one of the means of communication, which may be oral, written or by any other means. It is one of a communication that reaches, or is sure to reach, the public.

Thus it is not an invasion of the right of privacy, within the rule stated in this Section, to communicate a fact concerning the plaintiff's private life to a single person or even to a small group of persons. On the other hand, any publication in a newspaper or a magazine, even of small circulation, or in a handbill distributed to a large number of persons, or any broadcast over the radio, or statement made in an address to a large audience, is sufficient to give publicity within the meaning of the term as it is used in this Section. The distinction, in other words, is one between private and public communication.

Rest. (2d) of Torts § 652D, Comment a (1977).

Plaintiffs argue that they satisfy this standard because their address books were transmitted in an unencrypted manner, or over public WiFi, “making it publicly available to third parties as well as service providers.” ECF No. 422 at 27. That argument fails to meet the disclosure requirement for this claim. While Plaintiffs allege that their information could have been intercepted by third parties, they do not allege that any interception occurred, nor do they allege that it was “substantially certain” that their address books would become “public knowledge.” To

1 satisfy the requirement, more specific allegations establishing the extent of the disclosure are
2 required.

3 For this reason, the Court will dismiss the Opperman Plaintiffs' public disclosure claim.

4 **E. CDAFA and Computer Fraud and Abuse Act**

5 The Court's analysis *supra*, Part III.D, concerning the California Comprehensive
6 Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502, applies equally to
7 Plaintiffs' claims against the App Defendants. For the challenged conduct to qualify as "without
8 permission" under the CDAFA, the conduct must involve circumventing "restrictions on access"
9 of some kind. The CAC does not allege that the subject apps circumvented any restrictions.

10 Plaintiffs also assert a claim for violation of the federal Computer Fraud and Abuse Act
11 ("CFAA"), 18 U.S.C. §§ 1030(a)(2)(C), (a)(5), & (g), against the App Defendants. Plaintiffs
12 concede that, like the CDAFA, the CFAA applies only to a defendant's access to a computer
13 "without authorization," and that this limitation must be interpreted similarly to the "without
14 permission" language in the CDAFA. *See, e.g., iPhone I*, 2011 WL 4403963, at *11 ("Where the
15 software that allegedly harmed the phone was voluntarily downloaded by the user, other courts in
16 this District and elsewhere have reasoned that users would have serious difficulty pleading a
17 CFAA violation.").

18 Plaintiffs do not advance any new arguments concerning the "without authorization"
19 limitation in the CFAA, relying instead on their arguments concerning the CDAFA.
20 Consequently, the Court will dismiss both claims.

21 **F. Electronic Communications Privacy Act**

22 The Federal Wiretap Act, or Electronic Communications Privacy Act ("ECPA"), 18 U.S.C.
23 § 2510, prohibits "interception" of "wire, oral, or electronic communications." *Id.* § 2511(1). The
24 Act provides a private right of action against any person who "intentionally intercepts, endeavors
25 to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or
26 electronic communication," *id.* § 2511(1)(a), or who "intentionally uses, or endeavors to use, the
27 contents of any wire, oral, or electronic communication, knowing or having reason to know that
28 the information was obtained through the interception of a wire, oral, or electronic communication

in violation of [the Wiretap Act],” id. § 2511(1)(d). “Intercept” is defined as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” Id. § 2510.

All Plaintiffs except Pirozzi assert an ECPA claim against the App Defendants. Judge Gonzalez Rogers previously dismissed the ECPA claim in Hernandez for the same reason the App Defendants seeks dismissal here: “The FAC fails to allege that Defendant intercepted any communication contemporaneously with its transmission. Although Path allegedly transmitted the Class Members' Contact Address Books from the Class Members' mobile devices to Path's servers, Path did not ‘intercept’ a ‘communication’ to do so.” Hernandez, 2012 WL 5194120, at *3. Similarly, the Ninth Circuit has noted that “‘interception’ means “‘communication contemporaneous with transmission.’” Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004) (quoting Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002) (holding unauthorized access to e-mail messages did not violate ECPA). “Specifically, Congress did not intend for ‘intercept’ to apply to ‘electronic communications’ when those communications are in ‘electronic storage.’” Id. (internal quotation marks omitted) (quoting Konop, 302 F.3d at 876).

Plaintiffs simultaneously “preserv[e] their disagreement with this court-generated rule in the event it is later overturned,” ECF No. 422 at 24, and also advance the tortured argument that the contemporaneous interception requirement is met here because the apps in question caused Plaintiffs’ iDevices to “send information from the user’s Contacts from the iDevice’s storage memory to processors and active memory being used by the app” and then “simultaneously intercept[ed] that transmission.” Id. The decisions in Konop and Theofel are dispositive. In those cases, the “transmission” Plaintiffs describe here as being “intercepted” —the use of data by different memory components of the same device — was insufficient to give rise to an ECPA claim. The Court will dismiss Plaintiffs’ ECPA claim.

G. Texas and California Wiretap Statutes

Plaintiffs’ claims under the California Invasion of Privacy Act, Cal. Pen. Code § 630, and the Texas Wiretap Acts, Tex. Code Crim. Proc. Art. 18.20, § 1(3) & Tex. Pen. Code § 16.02(A), state analogues to the ECPA, suffer from the same deficiency as their federal claim. Indeed,

Plaintiffs incorporate by reference their arguments concerning the ECPA with respect to those claims, and do not present any other argument concerning the “interception” requirement in the Texas and California statutes. The Court will dismiss those claims for the same reasons. See, e.g., Hernandez, 2012 WL 5194120, at *5.

H. Texas Theft Liability Act

The Texas Plaintiffs assert a claim for violation of Texas Penal Code section 31.03(a), which provides that a person commits theft: “if he unlawfully appropriates property with intent to deprive the owner of property.” “Deprive” means “(A) to withhold property from the owner permanently or for so extended a period of time that a major portion of the value or enjoyment of the property is lost to the owner; (B) to restore property only upon payment of reward or other compensation; or (C) to dispose of property in a manner that makes recovery of the property by the owner unlikely.” Tex. Pen. Code § 31.01(2)(A)–(C).

Plaintiffs cannot satisfy the definition of “deprive” for purposes of their Texas Theft Liability Act claim. Even if Plaintiffs have a property right in their address books, there is no allegation that the App Defendants withheld the address books from Plaintiffs “permanently or for so extended a period of time that a major portion of the value or enjoyment of the property” was lost. Nor do Plaintiffs allege that the App Defendants offered to restore the address books for payment, because no restoration is possible; the address books were copied. For the same reason, Plaintiffs have not alleged that the App Defendants disposed of the property. Consequently, the Court will dismiss the Texas Plaintiffs’ Texas Theft Liability Act claim.

I. RICO and Vicarious Liability

Plaintiffs “elect not to prosecute [their RICO and vicarious liability] claims at this time and have no objection to their dismissal without prejudice as to” the App Defendants. As discussed above with respect to Plaintiffs’ RICO claim against Apple, the Court construes Plaintiffs’ statement as a Rule 41(a)(1)(A)(i) notice of voluntary dismissal, which is self-executing.

V. FACEBOOK AND GOWALLA’S MOTION TO DISMISS

App Defendants Facebook and Gowalla move to dismiss Plaintiffs’ claims against them for violation of the Uniform Fraudulent Transfer Act (“UFTA”), Cal. Civ. Code § 3439, *et seq.*,

1 for common law aiding and abetting, and for successor liability (as against Facebook only).

2 Plaintiffs allege that “[i]n late 2011, Facebook conducted due diligence on Gowalla for a
3 contemplated business transaction with Gowalla and/or Gowalla’s owners. The contemplated
4 transaction involved transfer of all or substantially all of Gowalla’s assets, technology, know-how
5 or equity to Facebook.” CAC ¶ 414. According to the CAC, Facebook discovered that Gowalla’s
6 app had been copying users’ address books without consent and decided as a result to structure the
7 transaction differently. The resulting transaction transferred to Facebook Gowalla’s key
8 personnel, “technology” and “know-how.” CAC ¶ 416. “Facebook did not pay Gowalla
9 reasonably fair value for the Gowalla assets, technology, know-how or personnel. Facebook
10 instead paid Gowalla’s shareholders and management for the company’s assets. On information
11 and belief, Facebook made payments of cash and/or Facebook pre-IPO stock to Gowalla’s
12 stockholders and management (instead of Gowalla) in consideration for this transaction.” CAC ¶
13 417. The transaction left Gowalla “effectively headless, lacking independent (or any) continuing
14 management, and insolvent” CAC ¶ 418.

15 The transaction was memorialized in a Release and Waiver Agreement submitted to the
16 Court under seal by Facebook and Gowalla.²⁴ The Agreement demonstrates that Facebook
17 transferred a substantial amount of cash and pre-IPO shares to Gowalla, not to Gowalla’s
18 shareholders or owners. The Agreement also conveyed to Facebook a non-exclusive, royalty-free
19 license to Gowalla’s patents. It did not convey title to any of Gowalla’s intellectual property.
20 Finally, the Agreement permitted Gowalla to redistribute the shares Gowalla received under
21 certain conditions. Plaintiffs point out that the Agreement refers to several documents that are not
22 in the record, and that the Agreement does not provide the Court with any information concerning
23 how the contract was performed.

24 **A. Uniform Fraudulent Transfer Act**

25 “The [California] UFTA permits defrauded creditors to reach property in the hands of a
26

27 ²⁴ Because the CAC depends on the transaction at issue, the Court hereby takes judicial notice of
28 the Agreement. See Swartz v. KPMG, LLP, 476 F.3d 756, 763 (9th Cir. 2007).

transferee.” Fid. Nat. Title Ins. Co. v. Schroeder, 179 Cal. App. 4th 834, 840–41 (2009). “A fraudulent conveyance under the UFTA involves ‘a transfer by the debtor of property to a third person undertaken with the intent to prevent a creditor from reaching that interest to satisfy its claim.’” Filip v. Bucurenciu, 129 Cal. App. 4th 825, 829 (2005) (quoting Kirkeby v. Super. Ct., 33 Cal. 4th 642, 648 (2004)).

Under the California UFTA,²⁵ a fraudulent transfer may be “actual” or “constructive.” Cal. Civ. Code § 3439.04(a). “In order for a fraudulent transfer to occur, among other things, there must be a *transfer* of an *asset* as defined in the UFTA.” Schroeder, 179 Cal. App. 4th at 841 (emphasis in original). Under the Act, “transfer” is defined as “every mode, direct or indirect, absolute or conditional, voluntary or involuntary, of disposing of or parting with an asset or an interest in an asset, and includes payment of money, release, lease, and creation of a lien or other encumbrance.” Cal. Civ. Code § 3439.01(i). An “asset” is, in turn, defined by the term “property,” which is defined as “anything that may be the subject of ownership.” Cal. Civ. Code § 3439.01(a), (h). A creditor cannot premise a UFTA claim on a transfer unless the “the transfer puts beyond [the creditor’s] reach property [the creditor] otherwise would be able to subject to the payment of [] debt.” Mehrtash v. Mehrtash, 93 Cal. App. 4th 75, 80 (2001).

In addition, to establish an “actual” fraudulent transfer claim under Civil Code § 3439.04(a)(1), Plaintiffs must plead that Gowalla made a transfer with “actual intent to hinder, delay, or defraud any creditor of the debtor.” Cal. Civ. Code § 3439.04(a)(1). When pleading these elements, Plaintiffs must meet the heightened standards mandated by Rule 9(b) of the Federal Rules of Civil Procedure. See In re SCI Real Estate Investments, LLC, No. 2:11-BK-15975-PC, 2013 WL 1829648 (Bankr. C.D. Cal. May 1, 2013).

²⁵ Facebook and Gowalla argue that Plaintiffs do not have standing to assert a California UFTA claim against them because they are not residents of California. The Court has already rejected that argument with respect to Apple’s motion to dismiss. Plaintiffs have standing to assert a California UFTA claim against Facebook and Gowalla, which are headquartered in California, for conduct that occurred in California.

As for the choice-of-law analysis, the parties agree that the California and Texas UFTA statutes do not conflict. Consequently, the Court will analyze California’s UFTA.

Here, Plaintiffs' allegations do not establish that any transfer of assets occurred within the meaning of the UFTA. Plaintiffs only describe generally what assets they assert were transferred: personnel, "technology," and "know-how." Plaintiffs fail to address the requirement that the transfer at issue put beyond Plaintiffs' reach property they otherwise would be able to subject to the payment of debt. There is no suggestion, for example, that Plaintiffs could not subject Gowalla's intellectual property, which Gowalla retained, to the payment of a future debt, or that the license Gowalla conveyed to Facebook somehow impaired its ability to satisfy creditor claims. Certainly Gowalla's employees are not "assets" for purposes of the UFTA. The parties have cited only one case to the Court on this point, Fink v. Advanced Logic Sys., Inc., A-5939-05T1, 2007 WL 3239222, at *7 (N.J. Super. Ct. App. Div. Nov. 5, 2007), and there, the court held that a non-exclusive license to copyrighted work was not an asset for purposes of a New Jersey fraudulent transfer.²⁶

Because Plaintiffs have failed to allege a transfer of assets within the meaning of the UFTA, their UFTA claim will be dismissed.

B. Successor Liability

Each claim asserted against Gowalla in this case is also asserted against Facebook by virtue of successor liability. Under California law, a corporation that purchases the assets of another does not assume the liabilities of the selling corporation unless: "(1) there is an express or implied agreement of assumption, (2) the transaction amounts to a consolidation or merger of the two corporations, (3) the purchasing corporation is a mere continuation of the seller, or (4) the transfer of assets to the purchaser is for the fraudulent purpose of escaping liability for the seller's debts." Ray v. Alad Corp., 19 Cal. 3d 22, 28 (1977). Plaintiffs' allegations on this point are materially deficient because they have not alleged that Facebook acquired Gowalla, and, as discussed above, they have failed to allege a transfer of assets. Indeed, the CAC expressly alleges the opposite: that Facebook acquired employees and intellectual property rights, but not Gowalla

²⁶ In briefing and at oral argument, Plaintiffs point to a Facebook securities filing and make other arguments based on facts not contained in the CAC. The Court declines to consider these arguments.

1 itself.

2 There is no successor liability where no acquisition or fraudulent transfer has occurred.
 3 See, e.g., Gee v. Tenneco, Inc., 615 F.2d 857, 862 (9th Cir. 1980) (“It is the general rule that
 4 where a corporation is not dissolved following a sale of assets or a reorganization, it remains liable
 5 for debts and liabilities incurred by it, unless it is otherwise agreed between the corporation and its
 6 creditors.”). Consequently, Plaintiffs have failed to plead any claims against Facebook by virtue
 7 of successor liability.

8 **C. Aiding and Abetting**

9 Facebook argues, and Plaintiffs do not contest, that Texas law applies to Plaintiffs’ claims
 10 against it. ECF No. 394 at 6 n.6; ECF No. 434 at 2. Texas does not recognize a claim for “aiding
 11 and abetting” as alleged in the CAC.

12 In Juhl v. Airington, 936 S.W.2d 640, 643 (Tex. 1996), the Texas Supreme Court declined
 13 to adopt section 876 of the Restatement (Second) of Torts, which sets out a “concerted action”
 14 theory of liability, noting that whether concerted action liability is recognized in Texas would
 15 remain an “open question.”²⁷ No subsequent case, however, has ever allowed such a claim. See
 16 Eckhardt v. Qualitest Pharm. Inc., 858 F. Supp. 2d 792, 802 (S.D. Tex. 2012) (“It is an ‘open
 17

18 ²⁷ Section 876 of the Restatement provides:

19 For harm resulting to a third person from the tortious conduct of
 20 another, one is subject to liability if he

21 (a) does a tortious act in concert with the other or pursuant to a
 22 common design with him, or

23 (b) knows that the other's conduct constitutes a breach of duty and
 24 gives substantial assistance or encouragement to the other so to
 25 conduct himself, or

26 (c) gives substantial assistance to the other in accomplishing a
 27 tortious result and his own conduct, separately considered,
 28 constitutes a breach of duty to the third person.

Rest. (2d) of Torts, § 876 (1977).

question' whether Texas law would even allow liability to be imposed based on § 876, and Plaintiffs have not directed the Court to any Texas cases holding a defendant liable under § 876. It is not the role of this Court, 'Erie-bound,' to expand Texas tort law.'').²⁸


Plaintiffs' aiding and abetting claim will be dismissed.

VI. CONCLUSION

For the foregoing reasons, the Court hereby DISMISSES all of Plaintiffs' claims against all Defendants with leave to amend, with the exception of the Opperman Plaintiffs' claim for common law intrusion upon seclusion against the App Defendants. Plaintiffs have leave to file an amended complaint within thirty days from the date of this Order.

IT IS SO ORDERED.

Dated: May 14, 2014


JON S. TIGAR
United States District Judge

²⁸ Plaintiffs argue that because there is no case expressly *prohibiting* such a claim, Facebook's motion to dismiss should be denied. This California federal court will decline Plaintiffs' invitation to create new causes of action under the state law of Texas.